University of KwaZulu-Natal

Master Thesis

Characterisation of Polarisation–Entangled Photon Source for Quantum Key Distribution

Samah S. Abu Ali Fadol

June 2016

University of KwaZulu-Natal

Master Thesis

Characterisation of Polarisation–Entangled Photon Source for Quantum Key Distribution

Author:
Samah S. Abu Ali Fadol

A thesis submitted in fulfilment of the requirements for the degree of Master of Science

in the

School of Chemistry and Physics,
University of Kwazulu-Natal
Durban

As candidate's Supervisor, I have afford this dissertation for submission:

Supervisors: *Date & Signature:*

Dr. Yaseera Ismail _____

Prof. Francesco Petruccione _____

June 2016

Abstract

Entanglement in real physical systems has been of great interest due to its importance in quantum mechanics. It has applications related to quantum information science specifically quantum cryptography since it eliminates the possibility of photon number splitting attack during the key distribution process (Quantum Key Distribution). This thesis deals with creation, detection and characterisation of the correlated polarised photon pairs, which were emitted from a nonlinear BBO crystal via Spontaneous Parametric Down Conversion (SPDC) process. The procedure that leads to the construction of a polarisation-based entangled system is discussed by considering some of the measurement techniques, which can be applied to study fundamental quantum mechanics and its applications in quantum communication. This thesis consists of a set of experiments to validate the entanglement of single photon pairs. The first experiment realised by generating of polarised based entangled photon pairs. The quantum correlation between the entangled photon pairs have been tested by measuring the visibility of the system and by verifying the maximal violation of CHSH (Clauser, Horne, Shimony and Holt) inequality. In the second experiment, the fidelity of the system has been measured by carrying out the state tomography to reconstruct the two-photon density matrix and consider the interference effect of two photons. This helps to study the preservation of the quantum state during the propagation.

Declaration of Authorship

I, Samah S. Abu Ali Fadol, student number: 215082171
declare that this thesis titled, 'Characterisation of Polarisation – Entangled Photon Source for Quantum Key Distribution' and the work presented in it are my own. I confirm that:

- This research reported in this thesis, except where otherwise indicated, is my original research.
- This thesis does not contain other persons data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.
- This thesis does not contain other person's writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
  - Their words have been re-written but the general information attributed to them has been referenced.
  - Where their exact words have been used, then their writing has been placed in italics and inside quotation marks, and referenced.
- This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the references section.

Signed: _____

Date: _____

"If Quantum Mechanics has not profoundly shocked you, you have not understood it yet."

Niels Bohr

Acknowledgements

I would like to express my special appreciation and thanks to my advisors Professor Francesco Petruccione and Dr. Yaseera Ismail. Prof. F. Petruccione, you have been a tremendous mentor for me. I would like to thank you for encouraging my research and for allowing me to grow as a research scientist. Your advice on both research as well as on my career has been priceless. I am also very grateful for your patience, motivation, enthusiasm, and the great knowledge that you have in Quantum technology in general. I especially want to thank my Co. Supervisor, Dr.Yaseera Ismail, whose support and guidance made my thesis work possible. She has been actively helpful in my experimental work and has always been available to advise me. I would like to extend my thanks to Prof. Mark Tame for his guidance and recommendations on the exprimental work which made the measurements more accurate.

I also thank all my colleagues and the postgraduate students at the school of Chemistry and Physics at UKZN, Dr. M. Mariola, Ms. M. Schuld, Ms. S. Pillay and Mr. S. A. Uriri for sharing their knowledge with me in my project. Special thanks to Ms. M. Schuld and Ms. S. Pillay for the discussions, advice, that they shared with me in general throughout my research, specially M. Schuld for reading through my thesis couple of times. I should not forget to thank my friend Ms. Dina Osman for her support when I started the degree together with grammatical corrections to the thesis in general.

I thank the National Research Foundation (NRF) South Africa for financial support. I also would like to thank the Center of Quantum Technology group at UKZN for providing a great environment for me to learn more about the field in general, the interactions that I experienced during group meetings and seminars are priceless.

Special thanks to my family. Words cannot express how grateful I am to my mother, father, brothers for all of the sacrifices that you have made on my behalf. Your prayer for is what has sustained me thus far. A very special thanks to my lovely husband Aymen and my daughter Shahd for always being there for me.

Dedicated to my family.

Contents

List of Figures

List of Tables

Abbreviations

QKD	**Q**uantum **K**ey **D**istribution
BB84	**B**ennett **B**rassard 19**84**
E91	**E**kert 19**91**
EPR	**E**instein **P**odolsky **R**osen
CHSH	**C**lauser **H**orne **S**himony **H**olt
PNS	**P**hoton **N**umber **S**plitting
SPDC	**S**pontaneous **P**arametric **D**own **C**onversion
FWM	**F**our **W**ave **M**ixing
HVT	**H**idden **V**ariable **T**heory
LHV	**L**ocal **H**idden **V**ariable
BBO	β **B**arium **BO**rate
RSA	**R**ivest **S**hamir **A**dleman
SHG	**S**econd **H**armonic **G**eneration
HWP	**H**alf **W**ave **P**late
QWP	**Q**arter **W**ave **P**late
SPAD	**S**ingle **P**hoton **A**valanche **D**etector
FPGA	**F**ield **P**rogrammable **G**are **A**rray
CCU	**C**oincidence **C**ounting **U**nit
Lab VIEW	**Lab**oratory **V**irtual **I**nstrumentation **E**ngineering **W**orkbench

Chapter 1

Introduction

The theory of quantum mechanics is one of the most successful theories that governs our physical reality. It has been widely used in information exchange theories such as quantum information.

Quantum Key Distribution (QKD) is one of the most significant current applications in the field of quantum information theory. QKD is a method that uses the laws of quantum mechanics to guarantee the secret communication between two parties "The transmitter and the receiver", often called Alice and Bob, without any interception from a third party "Eve". A secretly distributed key is shared and exchanged between Alice and Bob to encode and decode the information. The security of the key is provided by the laws of the quantum mechanics instead of using complicated mathematical calculations as in the case of classical encoding (Moskovich, 2015).

QKD was first proposed as a communication protocol by Charles H. Bennett and Gilles Brassard in 1984, known as BB84 (Bennett and Brassard, 1984). This protocol is based on using photon polarisation states to achieve the security. QKD is unconditionally secure, since Eve can use any technology to hack the communication such as quantum computers and digital computers, but that is not enough to break QKD. To add more layers of privacy and security, an optimised setup like an entanglement-based quantum key distribution system is resistant to any eavesdropping attack (Waks *et al.*, 2002).

Entanglement occurs when two particles have been generated at the same time from the interaction of the particles in a nonlinear crystal. The properties of these particles will then remain connected in future times even if they are separated by a long distance.

The quantum state of the compound systems, in general, is inseparable (Dehlinger and Mitchell, 2002). Determination of the quantum state of one particle simultaneously determines the quantum state of the other particle irrespective of the distance between the particles. The measurement of the complete system of the entangled particle is always correlated.

The history of quantum entanglement is associated with the predictions of quantum mechanics which was first discussed in 1935 by Albert Einstein, in a joint paper with Boris Podolsky and Nathan Rosen, known as the Einstein-Podolsky-Rosen (EPR) paradox (Einstein *et al.*, 1935). In this paper they wrote "we are thus forced to conclude that the quantum-mechanical description of physical reality given by a wave functions is not complete". Like Einstein, Schrödinger was dissatisfied with the concept of the entanglement, because it seemed to violate the speed limit on the transmission of information, which is implicit with the theory of relativity (Schrödinger, 1936). Later, Einstein considered the entanglement as a feature of "spooky action at a distance". The discussion remained continuous for a long period until 1964, when John Stewart Bell (Bell, 1964) proposed an experiment involving the "hidden variable λ", that he added to complete quantum mechanics. Bell also demonstrated theoretically an inequality with a probability distribution. Soon after, Clauser, Horne, Shimony and Holt (CHSH) tested Bell's inequality experimentally by using pairs of polarisation entangled photons (Clauser *et al.*, 1969).

Quantum entanglement is one of the most significant phenomena in current quantum mechanics research with applications in communication, computing, biology and chemistry. In recent years, there has been an increasing interest in quantum entanglement, and it has become a fundamental physical concept in quantum information processing, such as quantum cryptography (Jennewein *et al.*, 2000), quantum teleportation (Bouwmeester *et al.*, 1997), quantum swapping (Pan *et al.*, 1998) as well as quantum computation (Horodecki *et al.*, 2009). QKD based on quantum entanglement was proposed by Ekert (1991). In this protocol, entangled particles from some source are received by Alice and Bob, who can measure and analyse the polarisation states along different basis. The security of the information is realised by violating CHSH inequality. Entanglement is also a basic theme in understanding many communication phenomena like secret sharing (Karlsson *et al.*, 1999), entanglement purification for quantum communication (Pan *et al.*, 2001), and dense coding (Mattle *et al.*, 1996).

Entanglement introduced new visions of considering many physical phenomena including, super-radiance (Lambert *et al.*, 2004), superconductivity (Berkley *et al.*), disordered systems (Serbyn *et al.*, 2013), and the emergence of classicality (Mascarenhas and Santos, 2009). There are a number of recent entanglement experiments: for example, multiphoton path entanglement which is created via the stimulated parametric down-conversion process (Eisenberg *et al.*, 2005), entanglement based quantum communication and violating of the Clauser-Horne-Shimony-Holt inequality measured by two observers separated by free space link 144 km (Ursin *et al.*, 2007), and the experimental purification of two-atom entanglement (Reichle *et al.*, 2006). Beside the aforementioned applications, entanglement between many photons (Zhao *et al.*, 2004), ions (Häffner *et al.*, 2005) and the entanglement between photon and an atom has been established (Volz *et al.*, 2005).

Currently, most of the applications involving QKD experiments are using a true single photon source, but that is impractical because it is generating the problem of Photon Number Splitting (PNS) attacks. Experiments using a single photon source produce highly attenuated light with a low photon rate, which leads to producing a photon in multi-photon bunches. This makes the intercepts much easier for Eve by splitting off and storing a single photon while the parties receive the other photons without any effect on the polarisation of the photons (Jennewein *et al.*, 2000). An entanglement based QKD method eliminates the PNS attack because the likelihood of simultaneously producing two entangled photon pairs is very low, such that the effectiveness of a PNS attack is vastly reduced.

QKD based entangled photons use quantum states of entangled photon pairs that are generally generated in optical system to realise quantum communication. To build an optical system for the quantum communication, the structure of the optical system will necessitate sources of pure entangled optical states with high fidelity. In order to obtain such optimized sources, the first step is to generate entangled photons from an ultra brightness photon source. In this thesis, we use a process known as Spontaneous Parametric Down Conversion (SPDC). This is a method of generating entangled photon pairs, which was established by Burnham and Weinberg (1970). They demonstrated that by pumping photons through a nonlinear crystal, it is possible to split a photon into a single photon pair, known as a signal and an idler. This non-linear process conserves energy and momentum; in other words, the added energy of the split signal and idler is

equal to the energy of the pump photon. This also applies to the momentum. In 1988, Leonard Mandel revealed the first optical experiment that uses the optical SPDC to generate the entangled state (Ou and Mandel, 1988). Afterwards the scientist Yanhua Shih violated Bell's inequality by using the Mandel's experiment (Shih and Alley, 1988). There exist other methods of generating entanglement, for example through quantum dots, as proposed by Mark Reed in 1988 (Reed *et al.* (1988)), exploiting atomic cascades (Aspect *et al.*, 1981) and also by using fibre coupled to mix photons and to generate narrowband entangled photons (Aspect *et al.*, 1981, Fedrizzi *et al.*, 2007). Recently through the use of spontaneous Four-Wave Mixing (FWM) in micro-resonators (Helt *et al.*, 2010).

This thesis describes the development of an automated portable optical quantum entanglement device, used to generate and characterise a polarised entangled photon pairs for QKD. These photons are emitted from a nonlinear crystal via type-I SPDC. This portable device is designed to generate a high efficiency, photon-on-demand entanglement, and to enhance high-quality entangled photon pairs. The output of this device will be a commercial product, which can be used in the scientific research..

In this thesis, I give a brief review of entanglement of photons, based on photon field interactions. I will focus on generating polarised entangled photons through type-I SPDC. Type-I SPDC is useful to generate stable entangled photons as well as they are easy to be aligned properly. An type-I β Barium Borate (BBO) nonlinear crystal is used as SPDC source to overcome the decoherence limitation of the brightness of the SPCD-based entanglement source. Also, a crystal compensator is used to increase the brightness and increasing the fidelity of the system (Rangarajan *et al.*, 2010).

I report the characteristic of the polarised entangled photon system to implement QKD by testing the non-classical correlations from entangled photon pairs. This test is realised by measuring the visibility of the system in two different bases (rectilinear and diagonal basis), hence I verify the existence of the entangled photons by violating the CHSH inequality. I also describe the quantum state tomography technique to complete the characterisation of the entangled photon pairs from the SPDC source according to the polarisation degree of freedom and measuring the fidelity of the system (James *et al.*, 2001).

This thesis is structured as follows:

Chapter 2 provides an overview of the mathematical description of quantum mechanics, focusing on the representation of states and operators in Hilbert space, the techniques used to reconstruct the quantum state for a qubit. It also contains the difference between pure and mixed quantum states and the general properties of density matrix. Finally, composite states and tensor product are discussed.

Chapter 3 discusses the concept of entanglement in detail with a brief history of the theory, and the physical concept of the entanglement between two photons. We also review Bell's inequality and CHSH inequality. Additionally, some of the application of entanglement such as a quantum cryptography specifically known as QKD are discussed.

Chapter 4 presents a theoretical explanation to implement a polarisation entangled photon pair experiment. It includes the discussion of the creation of the correlated photon pairs via type-I SPDC process. We discuss the correlation relation which is realised by measuring the visibility of the system and the violation the CHSH inequality. Further more, we consider the fidelity of the system in order to test the purity of the generated entangled photons, that is accomplished by reconstructing the density matrix of the quantum state.

Chapter 5 provides the experimental setup that includes the components and the procedure for the preparation of polarised entangled state as well as the detection of these entangled photons through coincidence counts. The following step is to test the visibility of the system, followed by the violating of the CHSH inequality and performing the state tomography to reconstruct the density matrix. The results and analysis that proves entanglement are presented.

Chapter 6 provides a summary and conclusion together with the plans for future works.

Chapter 2

Basics Concepts of Quantum Mechanics

Chapter two provides a historical background and some basic concepts in quantum mechanics used as the foundation of the theory of quantum entanglement. It discusses in detail the mathematical representation of quantum mechanical systems, quantum state tomography, qubits, pure and mixed states, density matrix, and composite systems and tensor product.

2.1 Brief History of the Theory of Quantum Mechanics

It has been more than a century since the birth of quantum mechanics. It demonstrated great results in theoretical and experimental aspects of physics. The theory of quantum mechanics is based on the concept of quantum packets (quanta) to describe the behavior of matter and energy of subatomic particles such as electrons, atoms and molecules. This behavior is predictable by observing the interactions of matter and radiation (Gamow, 1966). Quantum theory is an accurate description when classical mechanics fails to describe microscopic systems. For example, quantum theory is needed to describe the observation of spectra of light emitted when heating gases.

The concept of quanta proposed by Max Planck suggests that light beam is composed of photons. These photons have both a wave-like and particle-like nature, which is called "duality" (Planck, 1957). His discovery led to the birth of quantum mechanics,

which it deals with the subatomic world (Planck and Kangro, 1972). Max Planck also postulated that energy can be emitted or absorbed by matter, realised by his famous Black Body Radiation experiment (Kuhn, 1978) (an ideal body that absorbs all the radiation without reflecting it). A quanta of energy E is related to frequency as follows,

$$E = h\nu, \tag{2.1}$$

where h is Planck's constant, and ν is the frequency of the quanta.

Another basic concept of quantum mechanics is the uncertainty principle, which was formulated in 1927 by Werner Heisenberg. It states that the position and the momentum of a subatomic particle cannot be measured simultaneously (Heisenberg, 1949). This means there has to be some cutoff between classical mechanics and a quantum system.

The mathematical description of quantum mechanics has been developed by Born, Pauli, Jordan and others, and is based on observable quantities. The above mentioned scientists were able to solve the non-trivial problem of a harmonic oscillator (Gamow, 1966). According to Dirac, all physical quantities can be represented by operators. Also, he established that the quantum state of a quantum system are vectors in a Hilbert space (Dirac, 1939).

Einstein and other scientists considered the incompleteness of this theory (Einstein *et al.*, 1935), since it was considered to be just an illustration for a system directed by a wave-particle equation. Also, they studied the applicability of the theory to work in the macroscopic scale.

There are a number of experimental set ups to show that quantum mechanic systems cannot be labeled by classical mechanics. One of these experiments is the Mach-Zehnder interferometer experiment (Rarity *et al.*, 1990), which is named after the physicists Ludwig Mach and Ludwig Zehnder. In this experiment, a photon is directed toward a beam splitter followed by two detectors placed in the path of the outcoming photon. The photon behaves like a particle when the outcoming photon is detected by one of the detectors, and it behaves like a wave when propagating through the beam splitters. Here the photon illustrates a phenomena known as wave-particle duality. This phenomena leads to the theory of the quantum entanglement (Bromley and Greiner, 2000). In the next section, we will introduce some of the mathematical description of quantum system.

2.2 Mathematical Representation of Quantum System

States and Operators in Hilbert Space

Quantum theory is a mathematical model of the physical world. In order to characterise the model we need to specify how quantum states and operators are represented. This section follows the notation in Griffiths (2003).

States

A state is a complete description of a physical system. In quantum mechanics, a state is represented by a unit vector in Hilbert Space $\mathcal{H}$ which is essentially a complex vector space with an inner product. It describes the statistical state of a quantum system.

The vectors in the Hilbert space are denoted by $|\psi\rangle$. The inner product of the state $|\psi\rangle$ with it is complex conjugate $\langle\phi|$ is written as $\langle\psi|\phi\rangle$. The aforementioned inner product has the following properties for the vectors $|\psi\rangle$ and $|\phi\rangle$ in $\mathcal{H}$,

- Positivity: $\langle\psi|\psi\rangle > 0$ for $|\psi\rangle = 0$.
- Linearity: $\langle\phi| \left(a\,|\psi_1\rangle + b\,|\psi_2\rangle\right) = a\,\langle\phi|\psi_1\rangle + b\,\langle\phi|\psi_2\rangle$.
- Symmetry: $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle$.

A pure quantum state can be defined by a state vector, a wave function, or a complete set of quantum numbers for a definite system (Hayashi *et al.*, 2014). The inner product for a vector $|\psi\rangle$ in Hilbert space with itself is greater than one with the property that it is complete in the normalization condition, given as,

$$||\psi||^2 = \langle\psi\ |\psi\rangle = 1.$$

In the case that the vector $|\psi\rangle$ is the zero vector, the inner product $\langle\psi\ |\psi\rangle = 0$

Operators

In quantum mechanics, observable physical quantities are represented by operators that are linear maps of the Hilbert Space $\mathcal{H}$ into itself. Here, three cases are defined:

Case 1: When the unit operator $\hat{I}$ (identity operator) acts on a state vector $|\psi\rangle$, the result is the same vector, such as,

$$\hat{I}\,|\psi\rangle = |\psi\rangle.$$

Case 2: A general operator $\hat{A}$ acting on $|\psi\rangle$ is defined to give another vector $|\psi'\rangle$ in the same Hilbert space,

$$\hat{A}\,|\psi\rangle = |\psi'\rangle.$$

Case 3: Operators can be linearly combined. Given two operators $\hat{A}$ and $\hat{B}$ acting on a state $|\psi\rangle$, the sum of these operators $a\hat{A} + b\hat{B}$ when applied to the state $|\psi\rangle$ is defined as,

$$[a\hat{A} + b\hat{B}]\,|\psi\rangle = a(\hat{A}\,|\psi\rangle) + b(\hat{B}\,|\psi\rangle),$$

where a, b are complex numbers.

Case 4: There are zero operators $\hat{0}$ which always gives the null vector as a result,

$$\hat{0}\,|\psi\rangle = |0\rangle.$$

2.3 Superposition principle

In quantum theory all possible measurement outcomes are modeled by a vector basis in a Hilbert space. The state is however not restricted to one of these basis vectors, but can be in a superposition, where it is specified that, any two (or more) quantum states can be added together ("superposed") and the result will be another quantum state. It also specifies that conversely, every quantum state can be represented as a sum of two or more other distinct states (Wilde, 2013). An example of the superposition is a two-level

atom (a qubit state), which is a linear superposition of the "basis states" $|0\rangle$ and $|1\rangle$, which can be defined as,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{2.2}$$

The main difference between qubit state $|\psi\rangle$ and a classical probability distribution is that the probabilities interfere in general.

2.4 Qubits

The indivisible unit of classical information is the bit, it takes one of the two possible values 0 or 1. The analogue in quantum information is the *qubit* - which is short for quantum bit.

Qubits are mathematical objects with specific properties which are realised in an actual physical system. The qubit state can be represented with two computational states $|0\rangle$ and $|1\rangle$ in Hilbert Space. These states are assumed to be normalized and orthogonal. It is also possible to form linear combinations of states, which are called superpositions (Nielsen and Chuang, 2010),

$$|\psi\rangle = \alpha\,|\psi\rangle + \beta\,|\psi\rangle\,, \tag{2.3}$$

where α and β are probability amplitudes, which are complex numbers and related through the normalization condition.

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.4}$$

In quantum mechanics a two-dimensional complex Hilbert space $\mathcal{H}$ is used for describing the angular momentum or "spin" of a spin-half particle (electron, proton) and also the polarisation of a photon, which then provides a physical representation of quantum system.
The following sections will present the spin and the polarisation for a qubit.

2.4.1 Spin $\frac{1}{2}$ Particles

In quantum mechanics, the simplest possible system is a two-level system such as an electron or proton. These two-level systems have an intrinsic angular momentum which is associated with a quantity called spin. When an electron is placed in a magnetic field, a certain amount of energy can make the electron exist in either the ground state or excited state referred as two discrete, quantized spin states: spin up $|\uparrow\rangle$ and spin down $|\downarrow\rangle$, which can be represented by $|0\rangle$ and $|1\rangle$, respectively.

In a case when the electron at the ground state absorbs slightly less energy than is required to flip it to the excited state, the result is a superposition of the spin up and down states of this electron and oriented in such a way that it lies between the two discrete directions (Nielsen and Chuang, 2010).

The single qubit can be represented by the Bloch sphere which is a three dimensional geometrical sphere. It provides a useful means of visualizing the state of the single qubit. The coefficients α and β can be written in terms of angles as,

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}(\sin\frac{\theta}{2}|1\rangle\right), \tag{2.5}$$

where θ, φ and γ are real numbers, the factor $e^{i\gamma}$ can be ignored as it has no observable effects, therefore Eq. (2.5) can be written as,

$$|\psi\rangle = \left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}(\sin\frac{\theta}{2}|1\rangle\right), \tag{2.6}$$

where the numbers θ and φ define a point on the unit Bloch sphere, see Fig. (2.1).

When an electron in a magnetic field is observed, the measurement of the qubit in a state $|\psi\rangle$, which is the superposition of the two states $|0\rangle$ and $|1\rangle$, will collapse to either $|0\rangle$ or $|1\rangle$, resulting in an output of the state of spin "up" or spin "down". This means that the information on coefficients α and β is essentially lost. In principle, the coefficients can be obtained experimentally only if infinitely identically prepared qubits were measured. The measurement probability for a qubit in the state $|\psi\rangle$, is given by,

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \tag{2.7}$$

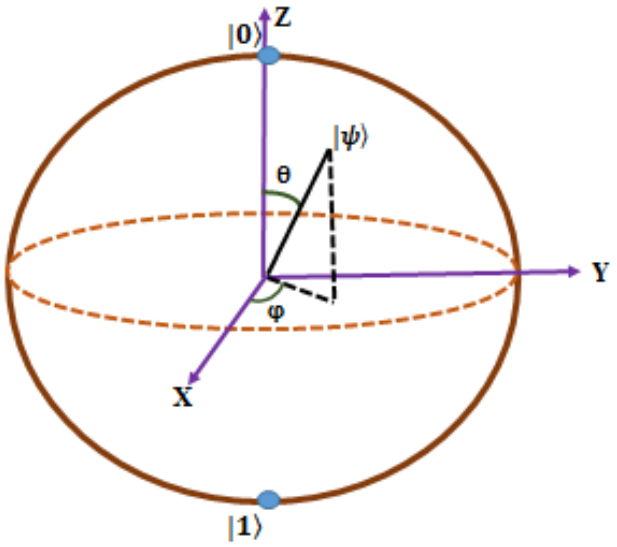


FIGURE 2.1: Bloch sphere representation for quantum mechanics system (qubit).

where by the state $|\psi\rangle$ has a 50% probability to collapse to either a state $|0\rangle$ or $|1\rangle$. The next section will present the polarisation for a qubit.

2.4.2 Polarisation

A photon is another important two state system which can have two independent polarisations. Photons are massless particles with spin-1. These polarisation states also transform under rotations, where their rotations about the axis is determined by their momentum. For a photon this corresponds to the familiar property of a light. The waves are polarised transverse to the direction of propagation.

Under a rotation about the axis of propagation, the two linear polarisation states $|H\rangle$ and $|V\rangle$ for horizontal and vertical polarisation respectively transform as follows,

$$|H\rangle \rightarrow \cos\theta\,|H\rangle + \sin\theta\,|V\rangle\,, \tag{2.8}$$

$$|V\rangle \rightarrow -\sin\theta\,|H\rangle + \cos\theta\,|V\rangle\,. \tag{2.9}$$

To describe the quantum interference phenomenon for the photon, suppose there is a polarisation analyser which allows only one of the two linear photon polarisations to pass through it. The polarised H or V photon then has a probability $\frac{1}{2}$ of getting through a 45° rotated polariser, and a polarised 45° photon has probability $\frac{1}{2}$ of getting through an H and V analyser (Zeilinger, 2010).

The polarisation analyser can be constructed easily in order to rotate the linear polarisation of a photon, and by applying the transformation Eq. (2.6) to a qubit. The relative phase of the two orthogonal linear polariation states are written as,

$$|H\rangle \rightarrow e^{\frac{i\varphi}{2}} |H\rangle , \tag{2.10}$$

$$|V\rangle \rightarrow e^{\frac{-i\varphi}{2}} |V\rangle . \tag{2.11}$$

2.5 Quantum State Tomography

Quantum State Tomography is the process of reconstructing the state of a quantum system by measurements based on multiple copies of the state by multiple modifications of the measurement apparatus.

The general principle behind quantum state tomography is determined by reconstructing the density matrix of the quantum system which is the best fit with the observations, by repeatedly performing different measurements on the quantum system. Coincidence counts can then be used to infer possibilities, and these possibilities which combined with Born's rule to determine a density matrix (Altepeter *et al.*, 2005).

George Stokes, in 1852, established the first experimental technique for determining the state of a system with his famous four parameter method. The method allows an experimenter to determine the polarisation state of a photon by considering coherent light beams with two-polarisation degrees of freedom. This makes the photon an ensemble of two level quantum mechanical systems. The Stokes parameters for such a system allows one to determine the density matrix describing this ensemble (Stokes, 2009).

In various experimental circumstances, the linear tomographic technique was devised in which the density matrix or Wigner function of a quantum state is found from a linear transformation of experimental data. The problem however, with this method

is that due to the experimental noise, the recovered state might not correspond to a physical state. The shortcoming with the Stokes parameter occurs because the density matrices for any quantum state must be hermitian and positive semidefinite unit trace.

An alternative method to reconstruct the density matrix of a physical system is the "maximum likelihood" tomographic approach. This method allows for the estimation and development of quantum states, thus avoiding the problem of the tomographically measured matrices which often fail to be positive semidefinite. The problem occurs when measuring low-entropy states, especially since the density matrix has produced a measured data set that is obtained by numerical optimization (James *et al.*, 2001).

The quantum state tomography technique has been successfully employed for the measurement of quantum systems for unknown quantum state. The next section will discuss pure and mixed states.

2.6 Mixed State and Density Matrix

Mixed State

The mixed state is the combination of probabilities that contain the information about the quantum state of the quantum system. A system is said to be in a mixed state if there is partial or no knowledge of the system. In terms of a probability density p , this means that more than one of its eigenvalues must be non-zero. A system can be describe by a mixed state when it is impossible to describe it by a state vector, except in the case that the state is not reducible to a convex combination of other statistical states, in which it is said to be in a pure state. The density matrix is a practical tool when dealing with mixed states. Typical mixed state refers to any case in which we subdivide a microscopic or macroscopic system into an ensemble, for which there is initially no phase relationship between the elements of the mixture. In general, for a mixed state, where the system is in the quantum-mechanical state $|\psi_i\rangle$ with probability ρ_i, the density matrix is the sum of the projectors, weighted with the appropriate probabilities (Hall, 2013).

In general, the mixed state can be considered as a collection of pure states $|\psi_i\rangle$, each with an associated probability p_i, with the conditions $0 \leq p_i \leq 1$ and $\sum_i p_i = 1$,

so the mixed state can then be written as the sum of pure state density matrices, as follows,

$$\rho = \sum_i p_i \rho_i^{\text{pure}} = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|. \tag{2.12}$$

The expectation value, can be defined as,

$$\langle A_{\rho_{\text{mix}}} \rangle = \text{Tr}(\rho_{\text{mix}} A). \tag{2.13}$$

The expectation value of the mixed state can be expressed as the sum of the expectation values of its constituent pure states, given as,

$$\langle A_{\rho_{\text{mix}}} \rangle = \sum_i \rho_i \left\langle\psi_i\right| A \left|\psi_i\right\rangle. \tag{2.14}$$

Density Matrix

In quantum theory, the density matrix or density operator ρ, acting on the Hilbert space are introduced to give a partial description of a quantum system. For example, the nee to construct a quantum description of subsystems, as composite quantum systems consist of two or more subsystems (Nielsen and Chuang, 2010). To represent systems by their density operator can be more useful and practical than the representation by state vectors.

For a physical system C in the pure state $\left|\psi_c\right\rangle$, the density operator of C equals the projector on this state, given by,

$$\rho_c = \left|\psi_c\right\rangle \left\langle\psi_c\right| . \tag{2.15}$$

To compute the expectation values from such a density operator for an observable A, the function is given by,

$$\langle A \rangle = \left\langle\psi\right| A \left|\psi\right\rangle . \tag{2.16}$$

The expectation values can be written as a trace of the observable, multiplied with the density operator, as follows,

$$\langle A \rangle = \left\langle\psi\right| A \left|\psi\right\rangle = \text{Tr} \left\langle\psi\right| A \left|\psi\right\rangle = \text{Tr}(\rho A). \tag{2.17}$$

General Properties of Density Matrices

For a pure quantum system found in state $|\psi\rangle$ with probability p , the density operator ρ for this system is defined as the outer product of the wave function and its conjugate. as we introduced in Eq. (2.15).

The density matrix is used to calculate the expectation value of any operator $\hat{A}$, which can be described as an observer A of the system. The density matrix is averaged over the different states $|\psi\rangle$. This is achieved by taking the trace of the product of ρ and A, that is defined by,

$$\left\langle \hat{A} \right\rangle = \mathrm{Tr}(\rho A). \tag{2.18}$$

The properties of the density matrix are as follows:

- Projector: $\rho^2 = \rho$ for pure state,
- Hermiticity: $\rho^\dagger = \rho$.
- Normalization: $\mathrm{Tr}(\rho^2) = 1$ for pure state , Tr $(\rho^2) < 1$ for mixed state.
- Positivity: $\rho \geq 0$.

The first property for the density matrix is no longer valid for the mixed state which can be defined by,

$$\rho^2_{\mathrm{mix}} = \sum_i \sum_j \rho_i \rho_j \, |\psi_i\rangle \, \langle\psi_i|\psi_j\rangle \, \langle\psi_j|, \tag{2.19}$$

where $\langle\psi_i|\psi_j\rangle = \delta_{ij} = 1$, hence Eq. (2.19) becomes,

$$\rho^2_{\mathrm{mix}} = \sum_i \sum_j \rho_i \rho_j \, |\psi_i\rangle \, \langle\psi_j| \neq \rho_{\mathrm{mix}}. \tag{2.20}$$

Thus far the quantum systems discussed involved only one particle. The next section introduces the case of more than one system, and the tensor product will be defined and explained.

2.7 Composite Systems And Tensor Product

A composite system is a system that consists of more than one particle, or the particle has internal degrees of freedom in addition to its center of mass.

If there is a composite system that involves numbered systems from 1 to 2, and system j is prepared in the state $|\psi_j\rangle$, the state of the composite system can be given as follows,

$$|\psi_1\rangle \otimes |\psi_2\rangle \,. \tag{2.21}$$

In quantum mechanics, the state space of a composite system from two different Hilbert spaces such as two qubits, is a tensor product of the Hilbert spaces of the component systems, where $\mathcal{H}_{ab} = \mathcal{H}_a \otimes \mathcal{H}_b$, and the symbol $\otimes$ denotes the tensor product.

For example, the tensor product of one particle in the Hilbert space is the tensor product of three spaces, each corresponding to the motion in one dimension (Griffiths, 2003). In case of a system composite of two Hilbert spaces $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$, their tensor product $A \otimes B$ can be obtained by assuming for simplicity that the space is finite dimensional. Let us consider $|a\rangle_j$ for $\{j = 1, 2\}$ to be an orthonormal basis consisting of a 2-dimensional system A, and $|b\rangle_p$ for $\{p = 1, 2\}$ to be an orthonormal basis consisting of a 2-dimensional system B, then the collection of the element of the system AB , is given by,

$$|a_j\rangle \otimes |b_p\rangle \ ,$$

where $|a_j\rangle = \sum_j a_j |a_j\rangle$, $|b_p\rangle = \sum_p b_p |b_p\rangle$. The Hilbert space $\mathcal{H}$ consists of all vectors that can be written in the form,

$$|\psi\rangle = \sum_j \sum_p N_{jp}(|a_j\rangle \otimes |b_p\rangle), \tag{2.22}$$

where N_{jp} are complex coefficient $= \alpha_j \beta_p$ in the case of the product state, Eq. (2.22) can be written as,

$$|a\rangle \otimes |b\rangle = \sum_j \sum_p \alpha_j \beta_p (|a_j\rangle \otimes |b_p\rangle). \tag{2.23}$$

In the product state, every element of $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ can be written in the form $|a_j\rangle \otimes |b_p\rangle$ such as Eq. (2.23). This means that the system A has the vector $|a\rangle$ and system B has

the vector $|b\rangle$. For example the product state of $(\ |a_1\rangle - |a_2\rangle\ ) \otimes (|b_1\rangle + \frac{1}{2}\,|b_2\rangle)$ is defined by,

$$|a_1\rangle \otimes |b_1\rangle + \frac{1}{2}\,|a_1\rangle \otimes |b_2\rangle_2 - |a_2\rangle \otimes |b_1\rangle\,| - \frac{1}{2}\,|a_2\rangle \otimes |b_2\rangle\,. \tag{2.24}$$

States which are not product states are said to be entangled, such that one cannot typically obtain definite properties of the individual systems A and B. In this case the complex coefficient $N_{jp} \neq \alpha_j \beta_p$. Nevertheless, if the state $|\psi\rangle$ is not representing an actual physical property, but representing the state as a "pre-probability", then the probabilities of the properties of the separate subsystems a and b can be given by using the same aforementioned example Eq. (2.24) and replacing the sign of the last term, the entangled state can be defined by,

$$|a_1\rangle \otimes |b_1\rangle + \frac{1}{2}\,|a_1\rangle \otimes |b_2\rangle - |a_2\rangle \otimes |b_1\rangle + \frac{1}{2}\,|a+2\rangle \otimes |b_2\rangle\,. \tag{2.25}$$

An example of entangled state is a two qubit system, and the state can be written as,

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|11\rangle\,, \tag{2.26}$$

where $\alpha \neq 0, \beta \neq 0$. In the next chapter we will discuss the entangled state in more detail.

Chapter 3

Quantum Entanglement Theory

Chapter three forms the literature review where the existing research on entanglement and QKD will be summarized. The chapter will discuss in detail the theory of Quantum Entanglement as well as some aspects of entanglement applications, such as Quantum Communication.

3.1 Quantum Entanglement

A pure state $|\psi\rangle$ is called separable if it can be written as $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. If is not seprable state means, it is an entangled state. An example for an inseparable state is $|00\rangle$. Typical example of entangled state are the Bell states, which are given by,

$$|\psi\pm\rangle = \frac{1}{\sqrt{2}} |00\rangle \pm |11\rangle . \tag{3.1}$$

$$|\phi\pm\rangle = \frac{1}{\sqrt{2}} |01\rangle \pm |10\rangle . \tag{3.2}$$

Entanglement is a physical phenomena that occurs when two subsystems particles generated or interacted at some point in time. The properties of these particles will then remain connected in future times even if they are separated by a long distance, and the quantum state of the compound systems is in general not separable. The determination of the quantum state of one particle simultaneously determines the quantum state of the other particle. Quantum entanglement has become a fundamental physical concept in quantum information processing and is used in quantum cryptography, quantum

teleportation, quantum error correction codes as well as quantum computation (Macchiavello *et al.*, 2001). Entanglement indicates a strong correlation between the entangled particles even after they are spatially separated. This correlation cannot be identified by classical mechanics.

3.2 The History of Quantum Entanglement

The history of entanglement theory is associated with the birth of the theory of quantum mechanics. The foundation of quantum entanglement demonstrated in 1930 by von Neumann, in which he proposed that the measurement of entangled photons, can be obtained without making use of the probability theory (Neumann, 1955). According to the standard "Copenhagen" interpretation of quantum mechanics, the measurement on the entangled photons state collapses into the basis, in which the measurement is carried out with the associated probabilities (Redhead, 1989). Von Neumann also presented the measurement of the collapsing state, which can be explained by entanglement of the measurement apparatus with the system that has been measured.

Schrödinger defined entanglement as a feature of quantum mechanics, by considering the entanglement between a macroscopic system (cat) and a microscopic object (atom). In 1935 He proposed a thought experiment as a discussion of the EPR paper. He described how to produce entanglement in a macroscopic system, in which the system depends on a quantum particle that was in a superposition. This thought experiment involves a cat that was put in a steel chamber together with a little amount of radioactive atom in a Geiger counter and it also contains a hammer and poison. The cat's life or death depends on whether radioactive atom had decayed and emitted radiation which will be detected with a Geiger counter. If the Geiger counter detects radiation, the hammer would crush the poison to kill the cat. According to the Copenhagen interpretation, the cat remains both alive and dead until the state is observed. An observer would see whether the cat was alive or dead according to the "superposition" principle. The fact that the cat was in a superposition state gives probability 50% of the state to collapse into either the complete knowledge that the cat is "alive" or "dead" but not both. This outward paradox is known as the Schrödinger cat paradox (Schrödinger, 1935).

" *In a complete theory there is an element corresponding to each element of reality*", this was stated by Einstein (Einstein *et al.*, 1935). In 1935, EPR designed a thought experiment "Gedankenexperiment" to suspect the incompleteness of quantum mechanics (Einstein *et al.*, 1935). EPR queried whether quantum theory could provide a full description of a physical reality in nature by considering the condition of the possibility of predicting the physical quantities with certainty, without disturbing the system. The logic of the experiment of EPR was as follows. For two particle system in a state $|\phi\rangle = \frac{1}{\sqrt{2}}|01\rangle \pm |10\rangle$, the measurement made on the first particle has an impact to the outcome on the second particle. After measurement of the first particle, the first particle is in a state $|0\rangle$ or $|1\rangle$ with probability $\frac{1}{2}$. The same results are obtained for the second particle. Suppose that the particles are separated from each other by millions of light years. If measuring the first particle it is obtained a state $|0\rangle$, then it is known that the second one is in a state $|1\rangle$. This means, the knowledge on the state of second particle came to the observer of the first particle faster than the speed of light. It follows that it is not satisfied at least in the principle of quantum mechanics.

Einstein came to the conclusion that some quantum effects travel faster than light, which is contradiction to the theory of relativity. They also concluded that by considering the problem of making predictions concerning a system, where the measurements made by another system that it had previously interacted with, leads to the result that these two systems cannot have a simultaneous reality (Mermin, 1985). This led to conclude that the description of reality as given by a wave function is not complete and this seemed somewhat paradoxical to Einstein. They were convinced that any complete physical theory must incorporate the principles of locality and reality.

EPR Locality and Realism, Locality is the idea that a physical state of one system can not be sufficiently separated. Performing any measurement to one system does not affect the other simultaneously; this means that there is no action at a distance whereby the measurement on a (sub) system does not affect the measurements on the other (sub) systems when they are far away from each other.

Realism, according to EPR is an element of physical reality corresponding to any physical quantity if the value of a physical quantity can be predicted with a probability equal to 1, without disturbing the system, hence the quantity has a physical reality. This seems paradoxical to the superposition principle, which state that the quantum

state is in state $|0\rangle$ or $|1\rangle$ with probability $\frac{1}{2}$. EPR maintained that, to explain quantum mechanics an "elements of reality" (hidden variables) must be added.

Hidden Variable Theory (HVT) is a theory similar to classical mechanics, which was proposed by Einstein to substitute quantum mechanics. Einstein believes in the completeness of this theory since it contained local interactions, which was implemented later by John Bell (Bell, 1966). The hidden variable element is defined as λ, and contains the missing information from quantum mechanics.

3.3 Bell's Theorem

3.3.1 Bell's Theorem and Bell's Inequality

John Stewart Bell originally proposed the idea for Bell's Theorem in his 1964 paper "On the Einstein Podolsky Rosen paradox" (Bell, 1964). In his analysis, he derived formulas called Bell inequality which concerned the conjecture that the Quantum Mechanical state of a system needs to be supplemented by further "elements of reality" or "hidden variables" or "complete states" in order to provide a complete description. The incompleteness of the quantum state was the explanation for the statistical character of Quantum Mechanical predictions concerning the system. In testing the inequality, it is the principle of locality that stands to fail rather than quantum mechanics. Indeed, tests of Bell's inequality have shown violations of the conditions to all Local Hidden Variable (LHV) theories.

3.3.2 Bell's Test Experiment

In the past many experiments have been carried out for testing Bell's inequalities by several scientists. In the mid of 1970's, Clauser, Freedman, Fry and Thompson created entangled states by using a radiative cascade of calcium, in which they had static analysers (Freedman and Clauser, 1972; Fry and Thompson, 1976). Also, in the 1980's, Aspect and his group used a very complex entangled source to generate polarised entangled photons, which was calcium atoms pumped by two separated lasers. The experimental results were compatible with quantum mechanics (Aspect *et al.*, 1981).

In the beginning of the 1990s, theoretical results were obtained in Bell inequalities violation by Alain Aspect, Philippe Grangier and Gerard Roger. They engaged two photon transitions of atomic cascade to create pairs of entangled photons (Aspect *et al.*, 1981).

In 1998, Zeilinger and his group provided an experiment for testing the Bell's inequalities, which showed that the distance did not break the entanglement (Weihs *et al.*, 1998). This experiment was achieved by using parametric down-conversion source and a β Barium Borate (BBO) crystal for producing the entangled states. They were able to send light through fiber couple optics over several kilometers distance. The results for this experiment were sufficiently good for quantum cryptography between two parties, Alice could not get any information from Bob with photons velocities less than the speed of light, and that established the condition of the Einstein locality.

Clauser, Horne, Shimony and Holt (CHSH) tested Bell's inequalities by using correlation pairs of polarisation entangled photons (Clauser *et al.*, 1969), which generalises Bell's inequality from the spin of the electron, used in the Bell's original proposal.

3.4 CHSH Inequality

In 1969 John Clauser, Michael Horne, Abner Shimony, and Richard Holt (CHSH) published a paper (Clauser *et al.*, 1969) in the form of the inequality to be used in the proof of Bell's theorem, which states that certain consequences of entanglement in quantum mechanics cannot be reproduced by local hidden variable theories.

Experimental verification of the violation of the inequalities is seen as experimental confirmation that nature cannot be described by local hidden variables. They derived the CHSH inequality, based on John Bell's original inequality. This inequality relates expectation values, that are obtained experimentally in a two-photon polarisation measurement. A violation of the CHSH inequality would violate human intuition as well, since it would imply that either locality or reality, if not both, must be rejected as fundamental features of nature. A detailed description of this test is reserved for the experimental part of this work.

The correlation quantity S is defines the CHSH inequality form, which is given by,

$$S = E(a, b) - E(a, b') + E(a', b) + E(a', b'), \tag{3.3}$$

where E is the quantum correlation of the photon pair. And a, a' and b, b' denote the local measurement settings of the two observers, respectively.

$$-2 \leq S \leq 2. \tag{3.4}$$

The mathematical formalism of quantum mechanics predicts a maximum value for S of $2\sqrt{2}$ which is greater than 2 as illustrated in CHSH Eq. (3.3), and violates the CHSH inequality.

The theory of entanglement attempts to give answers to fundamental questions such as; how entanglement can be created, characterised, detected and how to quantify entanglement theoretically and experimentally. These questions were answered by Werner and Popescu; Werner gives a precise definition of mixed separable states that are not entangled. He also noted that there exist entangled separable state that do not violate Bell's inequalities (Werner, 1989). Popescu found that the system in such a separable state, can be an entangled state by detecting the Bell's inequality when using of local operations and post coincidence (Popescu and Rohrlich, 1992). Later Gisin, developed Popescu's idea known as "filters" to enhance the violation of Bell inequalities (Gisin, 1991). The next section discuss in detail some of the application of the quantum entanglement.

3.5 Applications of Entanglement

Entanglement played a significant part in the development of quantum cryptography (Jennewein *et al.*, 2000), computing (Deutsch, 1985), teleportation (Bouwmeester *et al.*, 1997) and swapping (Pan *et al.*, 1998), which include the measurement based structures, one-way quantum protocol, and linear optics quantum computing.

Quantum cryptography was proposed by Stephen Wiesner in 1983, as a cryptosystem aimed to communicate information among parties without leaving chance of eavesdropping (Wiesner, 1983). He used the concept of the quantum state in the cryptography

to raise the security of the information. In this cryptosystem, two messages can be sent through a quantum channel, the receiver can repossess either one of the two messages but not both at the same time.

An extension to Wiesner's work, Charles Bennett and Gilles Brassard have developed a cryptosystem (protocol) in 1984. It is an application for QKD and it is known as BB84 (Bennett and Brassard, 1984). The original entanglement – based quantum cryptography protocol, proposed by Artur Ekert in 1991 is known as E91 protocol (Ekert, 1991). These protocols will be discussed in more detail in the next section.

Around the same period of developing quantum cryptography, quantum computation has been formalised by David Deutsch in 1985. Quantum computing is the science of using quantum mechanic theory for computing (Deutsch, 1985). While classical computers operate on digitised binaries called bits (0, 1), a quantum computer operates on a superposition of two-dimensional quantum bit known as "qubits" represented by the states $|0\rangle$, $|1\rangle$.

Quantum teleportation is another practice of quantum entanglement which was proposed by Bennett and his group in 1993 (Bennett *et al.*, 1993). It is the technique of sending a quantum state from one place to another, that demonstrated by using entangled photons and classical communication. In a simple illustration of this technique, the two parties Alice and Bob share a maximally pure entangled state, Alice is provided an unknown quantum state to be teleported to Bob, after Alice measured her state, the teleported unknown state will be provided by a Bell – basis measurement. Quantum swapping is a generalised theme for quantum teleportation since it can be applied to mixed entangled photons.

3.6 Entanglement and Quantum Communication

3.6.1 Cryptography and Protocols

Cryptography is the science of sending message between multiple people without allowing anyone to tamper the information. The purpose of a cryptographic protocol is to solve some problems including allowing multiple users to share information without letting anyone else know the constituents of the secret information.

Coding a message was traditionally one of the interests of military applications and spy agencies, that needed to get messages back to their headquarters. Nowadays cryptography becomes a fundamental part of everyone's life in ensuring secure connections such as credit card numbers needed to be transmitted securely over the Internet (Moskovich, 2015).

The simplest cryptographic task is sending a secret message between two parties, say from Alice to Bob, without any third parties, Eve, learning the contents of the message. A popular method used to encrypt the original message is public key cryptography. In this method, Bob first creates both a public key and private key, and publishes the public key over a public channel. Alice then uses Bob's public key to send him a secure message, in which she encrypts it by using the public key. Bob decrypts the message with his private key. Key generation is based on a calculation made by Bob, which is difficult to reverse by an eavesdropper— called Eve. The intended recipient applies a decryption rule utilizing the same key to this cyphertext in order to recover the original plaintext message (Gisin *et al.*, 2002).

Theoretically, the one-time pad protocol is the only way to ensure secure communications. This protocol uses a long random key shared securely between the parties and used only once. The problem of this approach is the key has to be distributed, which may be vulnerable to interception. Also reusing a one-time pad allows to code-breakers to find patterns that can reveal the key. RSA (Ron Rivest, Adi Shamir, and Leonard Adleman), which is one of the first practical public-key cryptosystems, is the standard classical method for solving these problems, in which Eve is limited computational power prevents her from factoring large numbers (Rivest *et al.*, 1978).

Another classical cryptographic protocol is the Bit commitment, in this protocol Alice chooses a bit randomly (0) or (1), and sends some of her choice to Bob, but he cannot know what Alice's bit choice is until she reveals it to him. Once she does, Bob can simply verify that she is telling the truth by using computational power. The unconditionally secure problem of this protocol realized when Bob is not able to determine the value of Alice's bit, which allows Alice to safely change the bit without Bob finding out. This led to a great disappointment, and later results proved that cryptographic protocols based on two quantum states (qubit) were possible (Goldreich, 2009).

The quantum method for ensuring the information is to secure the information without been decoded by an eavesdropper. To distribute a key that made of quantum channel, is hard to be intercepted without being detected by the sender or receiver. This is efficient because any act of measuring a quantum state by an eavesdropper will cause changes that can be detected and also because the measurements of the photon beam will cause detectable errors in the data.

QKD as we introduced previously, was proposed by Charles Bennett and Gilles Brassard. Their protocol is known as BB84 (Bennett and Brassard, 1984). The BB84 protocol uses the laws of quantum mechanics to ensure the security of the information between the parties by sharing a secret key in the form of qubits. For example, Alice generates a beam of polarised photons in one of two orthogonal basis: rectilinear (vertical /horizontal), or diagonal ($\pm 45°$), whereby each basis represents one orientation realised as bit "0" or "1". Alice randomly choses a basis and a bit for each photon sent over the quantum channel to Bob. Bob selects a basis randomly to measure the photon either rectilinear or diagonal without knowing the preprepared basis, after which he communicates with Alice over the public classical channel after he has measured all the photons. Bob reveals the basis being used, Alice confirms to keep or discard the bits based on basis selections.

The secret key will be generated by discarding the photon measurements (bits) when Bob uses a different basis as shown in Fig. (3.1). This process provides a secure quantum channel for key distribution because for Eve to eavesdrop the channel, She has to guess which basis to measure in. In the case, when Alice and Bob choose the same basis but the eavesdropper choses a different basis then the probability is 50% that Bob will measure a bit value different from what Alice sent, allowing Alice and Bob to detect an eavesdropper by publicly comparing and discarding a certain number of bits for which they chose the same basis.

The BB84 protocol was simplified by Charles Bennett in 1992 to the B92 protocol (Bennett, 1992). The coding in the B92 protocol uses two non-orthogonal states rather than the four polarisation states as in BB84 (Bennett and Brassard, 1984). For example, the bits "0" can be encoded as 45° on the diagonal basis while the bit "1" can be encoded by 0° in the rectilinear basis.

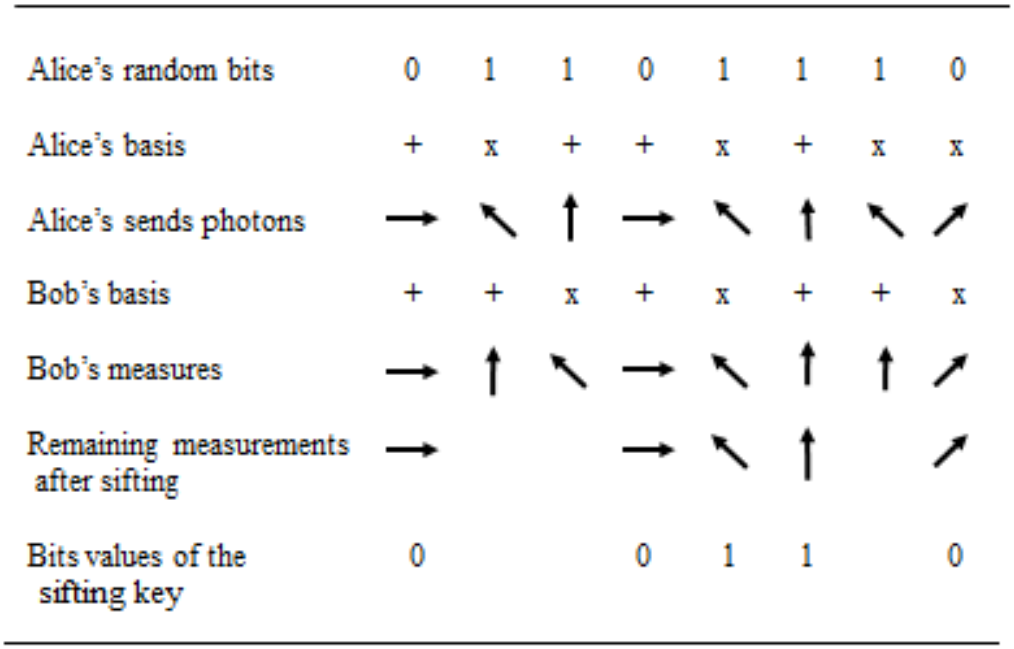


FIGURE 3.1: The figure shows the first Quantum key distribution protocol BB84 and how Alice and Bob measure their basis. Firstly, Alice chooses her bits randomly and her basis also to sent in to Bob. Bob chooses his basis and measures the incoming bits from Alice. The sifting key is composed from the remaining measurements.

In 1999, Pasquinucci and Gisin proposed another modification of BB84 protocol, which known as the Six-State Protocol (SSP) (Bechmann-Pasquinucci and Gisin, 1999). In SSP, the coding uses six states on three orthogonal bases. It is similar to BB84 except using six states rather than using two or four states. This protocol provides another layer of security because an eavesdropper would need to choose the right basis from a total of three bases and that produce a higher rate of error which can be easy to detect . The security of B92 protocol is was realised by using a single-photon source, which was demonstrated by Tamaki and Lütkenhaus, 2004.

The SARG04 protocol was proposed by Scarani, Acin, Ribordy, and Gisin in 2004 (Scarani *et al.*, 2004). This protocol shares the state sending phase and the measurement phase of BB84. Also, it uses the same four states and the same experimental measurement. The only difference between the two protocols is Alice does not directly reveal her bases to Bob, she reveals the non-orthogonal bases and Bob can measures his state with two possibilities, that his measurement is correct and that means he used the

right basis that Alice used to encode her bits, or he measured the incorrect basis and he will not be to determine Alice bits phase.
There are some other protocols that are not discussed in this study.

3.6.2 Entanglement Based QKD

Qubits are the basis for an entangled quantum system, they are generated from a single photon source to use them in quantum communication. The most commonly implemented entangled photon systems has been used in experimental demonstrations of various quantum communication protocols like teleportation, dense coding, and QKD (Jennewein *et al.*, 2000).

Entanglement based quantum communication was proposed by Artur Ekert in 1991 (E91) (Ekert, 1991). In the E91 protocol, the entangled states are perfectly correlated, which means if Alice and Bob both measure their photons with vertical or horizontal polarisations, they always get the same answer with 100% probability. However, Alice and Bob each receive half of an entangled photons, and by measuring the polarisation along different basis (similar to BB84 protocol). The results are completely random, which means it is impossible for Alice to predict if she (and thus Bob) will get vertical polarisation or horizontal polarisation. The security of this protocol is realised when Eve intercepts and resends anything, her measurement will break the entanglement between the photons and destroy the correlation in a way that Alice and Bob can easily detect (Lo and Lütkenhaus, 2007).

In Ekert's original paper, Alice and Bob would measure polarisation along three different angles. Alice would measure along 0°, 45°, and 90°, while Bob would measure along 45°, 90°, and 135°. As in BB84, they keep their series of basis choices secret until the measurements are completed. Then Alice and Bob publicly reveal the polarisation basis they used to measure. The measurement are carried out by making two groups of photons: The first one consists of photons measured using the same basis by Alice and Bob which is used as bits to generate the key while the second contains all other photons used to construct the the correlation quantity (S) that is used in the Clauser-Horne-Shimony-Holt (CHSH) inequality (Clauser *et al.*, 1969). By finding the quantity S, Alice and Bob could infer whether any eavesdropper had measured the polarisation state as

this would destroy entanglement and thus not allow violation of the CHSH inequality (Moskovich, 2015).

Anton Zeilinger, applied the E91 protocol by using a polarised entangled photon pair to demonstrate an Internet Banking Transfer over a distance of 1.4 km (Poppe *et al.*, 2004). The free space optical link together with the moving frame space link communication processes, was established by using entangled photons and the fidelity was successfully verified (Tapster *et al.*, 1994), (Aspelmeyer *et al.*, 2003).

Entanglement based QKD provides the possibility to obtain a secure key, which is provably secure against eavesdropping. Additionally, QKD can be composed with other encryptions, providing an additional secure layer for an already secure message. For example a message that was encrypted using the RSA cryptosystem, the public key can be encrypted again by using a quantum key. To intercept this message, an eavesdropper would have to break both the quantum key and the classical key. The capability distinguished by QKD from among all encryption methods it comes in the detection of eavesdropper where the measurements could be processed in different methods (Jennewein *et al.*, 2000).

Chapter 4

The Experiment Implementation

This chapter discusses the experimental implementation and the theory of generating a polarised-entangled photon pairs. The creation of entangled photon pairs via a non-linear SPDC process. Characterisation of the created polarised-entangled photon pairs, which can achieved by measuring the visibility of the system. The characterisation can be obtained by verifying the entanglement with violating Bell's Inequality as well as the measuring of the fidelity of system by testing the purity of the generated state.

4.1 Entangled Photon Pairs Production

The SPDC is a common scheme in the generation of entangled photon pairs. SPDC is a second order non-linear process involving the mixing of three electromagnetic waves. SPDC was first established in 1970 by D.C. Burnham and D.L. Weinberg, who implemented it by pumping photons at different points into the non-linear crystal. The photons that emerge from the crystal will split into singlet photons (Burnham and Weinberg, 1970).

4.1.1 Non-linear Optics

The interaction of a photon in a non-linear matter causes changes in frequency, the phase and the polarisation of the incident photon. The non-linear phenomena occurs when the photon travels through the material containing an optical field that depends

on a non-linear manner of the strength on the electric field $\tilde{E}(t)$. This produces a linear polarisation $\tilde{P}(t)$, which depends linearly on the behavior of the applied field, which is given by,

$$\tilde{P}(t) = \chi \tilde{E}(t), \tag{4.1}$$

where χ is the susceptibility coefficients, which is a tensor representing the relation between the polarisation vector and the product of the electric field vector.

For higher order electric field the material system can be described by the material polarisation, that is given by,

$$\tilde{P}(t) = \chi^{(1)}\tilde{E}(t) + \chi^{(2)}\tilde{E}(t)^2 + \chi^{(3)}\tilde{E}(t)^3 + ..., \tag{4.2}$$

where the $\chi^{(n)}$, $(n \neq 1)$ are the non-linear susceptibility coefficients, which depend on the direction of the electric field vector.

The main consideration to choose a crystal with large susceptibility is it high transmitting ability of the material for all wavelength ranges as well as the high resistance to laser damage. Another important requirement for choosing a crystal, is the good efficiency for the second-order nonlinear process such as SPDC. The phase matching of the incident and transmitted light waves is defined as,

$$\Delta K = k_s - k_2 - k_1 < \frac{1}{L} \tag{4.3}$$

where ΔK is the spatial variation in the wave function, L is the length of the material interaction region, k_s is the wave vector of the higher frequency, and k_1, k_2 are the wave vector of the other frequencies.

The phase matching condition that defined by the constructive interference cannot be easily satisfied that is because the refractive indices depend on the frequency, which results in some effects when using birefringence material.

Birefringence Material: Birefringence is a phenomena that is produced by a double value of refractive indices in uniaxial crystal, resulting in a rise of effects such as ordinary and extraordinary polarisation (Lin, 2013). When a crystal allows only one direction of propagation of light, the optical axis of the crystal z-axis, then is called an uniaxial crystal .

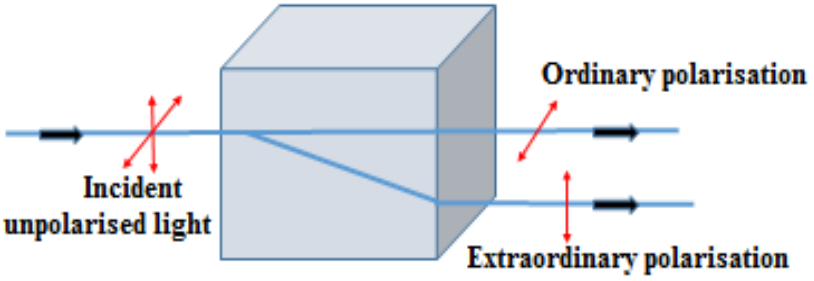


FIGURE 4.1: Illustration of the Ordinary and Extraordinary polarisation: unpolarised incident light pumping through a crystal and that emerges two kind of polarisations.

Ordinary and Extraordinary Polarisation: Ordinary and extraordinary polarisation are two types of polarisation resulting when an unpolarised pump light is directed towards a birefringent crystal, and splits into two rays. The two split rays represent the two types mentioned above, and illustrated in Fig. (4.1):

1. Ordinary (O) Polarisation: the split ray will have a polarisation in the direction perpendicular to the optical axis of the medium, also it follows Snell's Law to give a constant refractive index.

2. Extraordinary (E) polarisation: the split ray will have a polarisation in the direction of the optical axis of the medium, so that Snell's Law is not satisfied because it has a variable refractive index.

   The birefringence can be defined as the difference between the refractive index for the extraordinary polarisation n_e and the refractive index for the ordinary polarisation n_o,

$$\Delta n = n_e - n_o. \tag{4.4}$$

The positivity of the crystal is attained when $\Delta n > 0$, while $\Delta n < 0$ insure the negativity of the crystal.

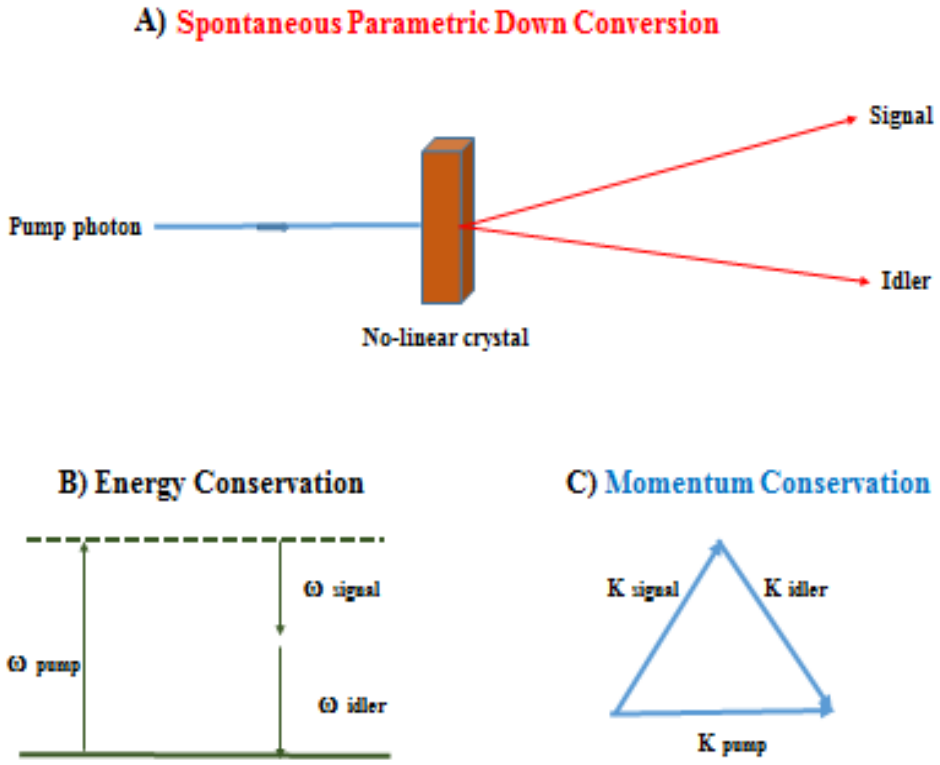


FIGURE 4.2: A) Spontaneous Parametric Down Conversion of the entangled photon pair is produced by pumping nonlinear crystal with photons. The emerged entangled photons are called signal and idler. B) The conservation of the momentum, C)the energy to generate the entangled photons are also illustrated.

4.1.2 Spontaneous Parametric Down Conversion

Spontaneous Parametric Down Conversion (SPDC) is a time-reversed process of Second Harmonic Generation (SHG), also referred to as parametric fluorescence or parametric scattering. It is a second-order non-linear process associated with the split of a high frequency photon into two lower frequency photons. It is a method to generate entangled photon pairs by pumping the incident photon through a non-linear crystal. The crystal lacks inversion of symmetry (de Dood *et al.*, 2004). The entangled photons are usually called the signal and the idler while the incident photon is called the pump photon. See Fig. (4.2).

SPDC is said to be "Spontaneous" because the signal and idler are generated spontaneously inside the crystal. It is "Parametric" since the process depends on the down-conversion of the photons electric field and their intensities. This results in a definite phase relation between the pump and entangled photons. "Down Conversion" means that the process of the split frequency of the pump photon producing entangled photons with lower frequencies (Beck, 2012). The entangled photons are produced at nearly the same time, and the individual photon properties are free to differ (Fox, 2006).

In SPDC, the splitting of the pump photon into two down-converted photons occurs in accordance with the conservation of energy and momentum of their single parent photon.

The energy conservation implies that the frequency of the signal and idler waves are added to each other, in which the energy of the pump photon is equal to the sum of the energies of the down-converted photons:

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i \tag{4.5}$$

$$\omega_p = \omega_s + \omega_i, \tag{4.6}$$

where $\hbar = \frac{h}{2\pi}, h$ is Plank's constant, ω_p, ω_s and ω_i are the frequencies of the pump, signal and idler photons.

The conservation of the momentum is equivalent to the phase matching, which requires,

$$k_p = k_s + k_i, \tag{4.7}$$

where k_p is the wave vector of the pump photon frequency, and k_s, k_i are the wave vector of the signal and idler photon frequencies respectively, see Fig. (4.2).

There are three types of SPDC of the down-converted process, that are characterised by the polarisation of the pump photon to produce entangled photons. Type-0 down conversion, Type-I down-conversion produces two down-converted photons with the same polarisation, but opposite to the pump photon. For type-II down-conversion, the down-converted photons have an orthogonal polarisation (Prutchi, 2012). Fig. (4.3) shows the difference between them.

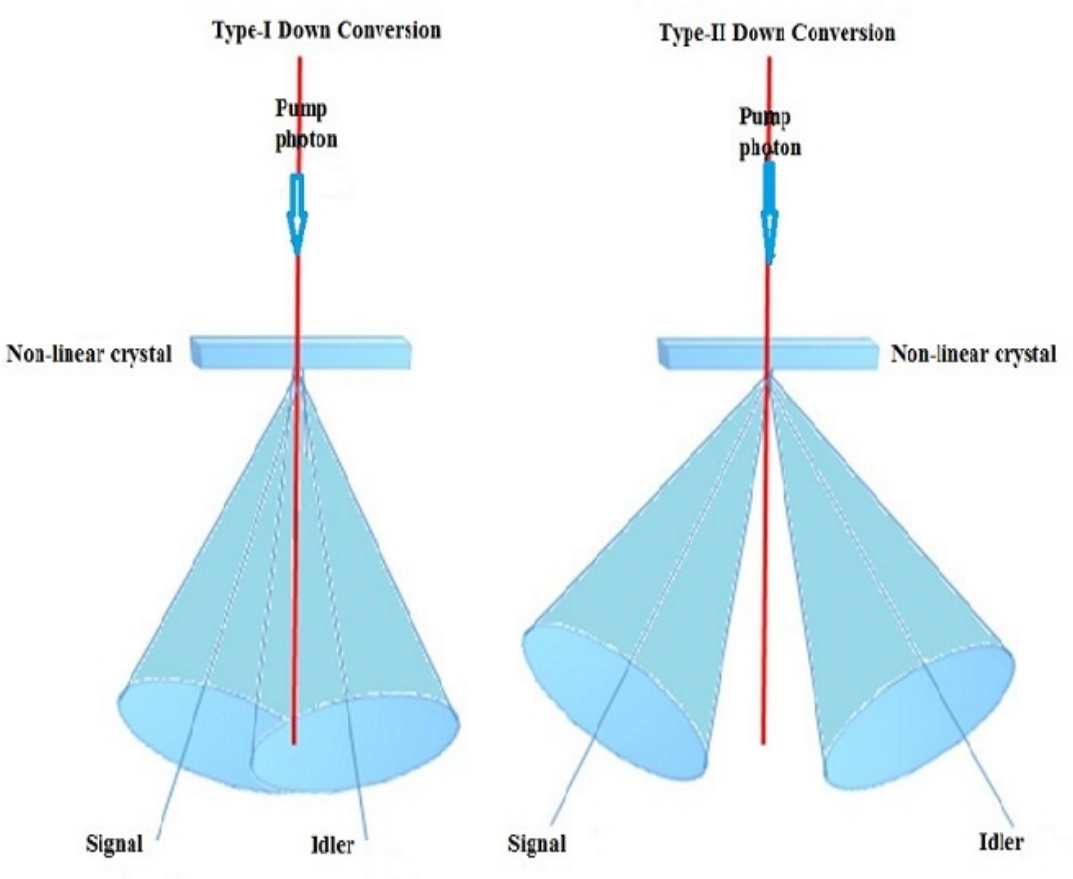


FIGURE 4.3: Type-I (right) and type-II (left) down conversion. The entangled photons emerging from type-I down conversion crystal will have the same polarisations that is opposite to the pump photon. And The entangled photons emerging from type-II down conversion crustal will have the orthogonal polarisations that is opposite to the pump photon.

The creation of the entangled photons via the SPDC process, allow us to study the fundamentals aspects of quantum mechanics. For example it allows to test the correlation between these photons and violating some classical theories such as Bell's inequality.

4.2 Correlation of Entangled Photon Pairs

The measurements on two qubits, that their entanglement state represented by Bell state in different basis, illustrated a perfect correlation when the qubits select the same basis.

4.2.1 Bell States

Bell states (sometimes called EPR states) are four specific maximally entangled quantum states of two qubits. Qubits are usually spatially separate, and they exhibit perfect correlation that cannot be explained without quantum mechanics (Kwiat *et al.*, 1995).

The four Bell States for polarised down converted photons are,

$$|\psi+\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle + |VV\rangle\right), \tag{4.8}$$

$$|\psi-\rangle = \frac{1}{\sqrt{2}}\left(|HH\rangle - |VV\rangle\right), \tag{4.9}$$

$$|\phi+\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle + |HV\rangle\right), \tag{4.10}$$

$$|\phi-\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle - |HV\rangle\right), \tag{4.11}$$

where H, V denoted to the Horizontal and Vertical polarisation respectively.

The Bell state defined in Eq. (4.8) and Eq. (4.9) can be written in the following equation,

$$|\psi\rangle_{Bell} = \frac{1}{\sqrt{2}}\left(|H\rangle_s |H\rangle_i \pm |V\rangle_s |V\rangle_i\right), \tag{4.12}$$

in which the indices s, i are for the signal and idler down converted photons respectively.

Bell state are defined the correlation of entangled states, in which the measurements on the outcome down converted photons in the vertical basis or horizontal basis, will have a $\frac{1}{2}$ probability for each basis. Also in case of taking the measurements at the same time for both of the down converted photons, the outcomes will appear random, but they are still correlated. This correlation helps the violation of local realism, because the measurement of one photon which is spatially separated from another photon does not influence the second photon.

4.2.2 The Polarisation State for Entangled Photon Pairs

The measurement of the polarisation state of the entangled photons, which are heading in different directions in the vertical and horizontal basis can be demonstrated by pumping a photon beam through a polariser with angle α, which gives rise to two possible results

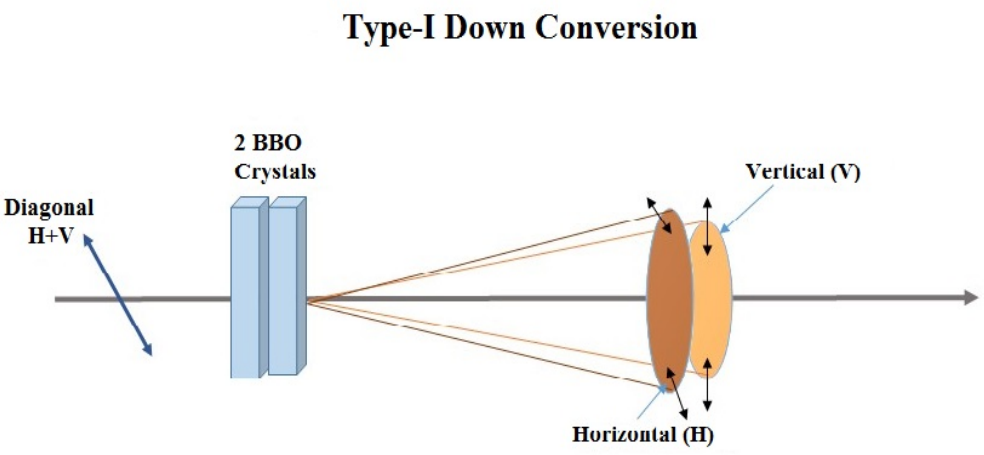


FIGURE 4.4: Two identical BBO crystals are cut for type-I down conversion, one oriented at 90° respected into the other, the cone shows the emission of the horizontal and vertical polarised photon pairs.

with 50% probability for each basis. In the case that the two photons are either both vertical states or horizontal states in terms of angle α, they are defined as follows,

$$|V_\alpha\rangle = \cos\alpha\,|V\rangle - \sin\alpha\,|H\rangle\,, \tag{4.13}$$

$$|H_\alpha\rangle = \sin\alpha\,|V\rangle + \cos\alpha\,|H\rangle\,, \tag{4.14}$$

The polarisation state for down converted photons generated from Bell state in Eq. (4.12) is given by,

$$|\psi\rangle_{\text{Bell}} = \frac{1}{\sqrt{2}}\left(|H_\alpha\rangle_s\,|H_\alpha\rangle_i \pm |V_\alpha\rangle_s\,|V_\alpha\rangle_i\right), \tag{4.15}$$

where $|V_\alpha\rangle$, $|H_\alpha\rangle$ are the polaristion state obtained after rotation of α from the vertical and horizontal basis respectively.

For the purpose of our experiment as will be shown later, the down converted photons were produced by using two identical BBO crystals, in which one is rotated 90° from the other, which have been cut to support type-I down conversion as represented in Fig. (4.4). Each crystal can support down conversion of one polarisation of the pump beam while the other polarisation can pass through the crystal with no change (Dehlinger and Mitchell, 2002).

The polarisation state of the pump photon in the input of the BBO crystal is given by:

$$|\psi\rangle = \cos\phi\,|H\rangle + \sin\phi\,|V\rangle\,, \tag{4.16}$$

when the pump photon is been absorbed by the first BBO crystal, the state reads:

$$|H\rangle \rightarrow |VV\rangle \equiv |V\rangle_s \otimes |V\rangle_i\,; \tag{4.17}$$

when the pump photon is been absorbed by the second BBO crystal, the state is:

$$|V\rangle \rightarrow |HH\rangle \equiv |H\rangle_s \otimes |H\rangle_i\,. \tag{4.18}$$

The state of the photon in the output of the two BBO crystals takes the form:

$$|\psi\rangle = \cos\phi\,|VV\rangle + \sin\phi\,|VV\rangle\,. \tag{4.19}$$

The polarisation states for the pump photon beam directed toward to the BBO crystal with despersion angle Δ, are given by,

$$|V_p\rangle \rightarrow |H\rangle_s\,|H\rangle_i\,, \tag{4.20}$$

$$|H_p\rangle \rightarrow e^{i\Delta}\,|V\rangle_s\,|V\rangle_i\,, \tag{4.21}$$

where the notation p, s and i, denoted the pump, signal and idler photons respectively, and Δ is the phase resulting from the dispersion in the crystal.

The polarised entangled photons can be generated by directing the pump beam through a linear polariser. The beam will create an angle θ from the vertical and the phase of the polarisation component ϕ_l will be shifted and that by using a birefringent quartz plate (Dehlinger and Mitchell, 2002). The polarisation of the pump beam is defined as,

$$|\psi_{\text{pump}}\rangle = \cos\theta_l\,|H\rangle_p + e^{i\phi_l}\sin\theta_l\,|V\rangle_p\,. \tag{4.22}$$

The polarisation of the state $|\psi_{DC}\rangle$ for the down converted photons after the pump beam reaching the crystal, is given by,

$$|\psi_{DC}\rangle = \cos\theta_l\,|H\rangle_s\,|H\rangle_i + e^{i\phi}\sin\theta_l\,|V\rangle_s\,|V\rangle_i\,, \tag{4.23}$$

where ϕ is defined as the phase difference of two polarisation components and given by $\phi = \phi_l + \Delta$.

In order to measure the polarisation states of the down converted photons, two polarisers rotated with angles α and β, are placed in the path of the signal and idler photons. Four possible outcomes can be detected: VV, VH, HV, HH (Geller, Dehlinger and Mitchell, 2002). The probability for detecting the vertical vertical (VV) basis is given by,

$$\begin{aligned} P_{VV}(\alpha,\beta) &= |\sin\alpha\sin\beta\cos\theta_l + e^{i\phi}\cos\alpha\cos\beta\sin\theta_l|^2 \\ &= \sin^2\alpha\sin^2\beta\cos^2\theta_l + \cos^2\alpha\cos^2\beta\sin^2\theta_l \\ &\quad + \frac{1}{4}\sin 2\alpha\sin 2\beta\sin 2\theta_l\cos\phi \\ &= \frac{1}{2}\cos^2(\alpha-\beta). \end{aligned} \tag{4.24}$$

The remaining probabilities of the polarisation combination for the horizontal horizontal (HH), vertical horizontal (VH) and horizontal vertical (HV) outcomes are defined as:

$$P_{HH}(\alpha,\beta) = \frac{1}{2}\cos^2(\alpha-\beta), \tag{4.25}$$

$$P_{VH}(\alpha,\beta) = \frac{1}{2}\sin^2(\alpha-\beta), \tag{4.26}$$

$$P_{HV}(\alpha,\beta) = \frac{1}{2}\sin^2(\alpha-\beta). \tag{4.27}$$

The experiment measures the coincidence counts $C(\alpha,\beta)$ for the signal and idler photon pair with polarisation angle α,β can be written as:

$$P_{VV}(\alpha,\beta) = \frac{C(\alpha,\beta)}{C_{\text{total}}}, \tag{4.28}$$

$$P_{HH}(\alpha,\beta) = \frac{C(\alpha_\perp,\beta_\perp)}{C_{\text{total}}}, \tag{4.29}$$

$$P_{VH}(\alpha,\beta) = \frac{C(\alpha,\beta_\perp)}{C_{\text{total}}}, \tag{4.30}$$

$$P_{HV}(\alpha,\beta) = \frac{C(\alpha_\perp,\beta)}{C_{\text{total}}}, \tag{4.31}$$

where $\alpha_\perp = \alpha + 90°$, $\beta_\perp = \beta + 90°$ and C_{total} is the total number of coincidence counts of photon detection, which is defined as:

$$C_{\text{total}} = C(\alpha, \beta) + C(\alpha_\perp, \beta_\perp) + C(\alpha, \beta_\perp) + C(\alpha_\perp, \beta). \tag{4.32}$$

4.2.3 Correlation and CHSH Inequality Violation

The entangled states must demonstrate a perfect correlation, which is independent of the basis when the measurement is carried out. The measurements are performed in a given basis (orthogonal basis) and if the correlation is found; the same measurements can be repeated in a different bases (orthogonal and diagonal bases) to check whether or not the correlation still exists.

Experimentally, the determination of the correlation of the entangled photon pairs can be achieved by testing the visibility in a different basis (Dehlinger and Mitchell, 2002). The visibility is given by,

$$V = \frac{C_{\text{max}} - C_{\text{min}}}{C_{\text{max}} + C_{\text{min}}}, \tag{4.33}$$

where V is the visibility, C_{max} and C_{min} are the maximum and minimum coincidence rates of detecting the entangled states respectively. To satisfy the condition of observing the entangled state, the visibility must be larger than $\frac{1}{\sqrt{2}}$.

By applying the Gaussian error propagation rule, the error in calculating the visibility (ΔV) can be given as:

$$\Delta V = \sqrt{(\frac{\partial V}{\partial C_{\text{max}}}\Delta C_{\text{max}})^2 + (\frac{\partial V}{\partial C_{\text{min}}}\Delta C_{\text{min}})^2}. \tag{4.34}$$

After observing the visibility, another measurement had to be performed to violate Bell's inequality to verify the entanglement.

The experimental realisation of Bell's Inequality (Bell, 1964), presented by Clauser-Horne-Shimony-Holt (CHSH) Inequality (Clauser *et al.*, 1969), showed a classical argument that limits the correlation of two polarised photons under measurements at different polarisers angles.

The CHSH Inequality uses a correlation of the probabilities, which can be defined by two measurement quantities, the correlation function E and the quantity S. The correlation function is given by,

$$\begin{aligned} E(\alpha,\beta) &= P_{VV}(\alpha,\beta) + P_{HH}V(\alpha,\beta) - P_{VH}(\alpha,\beta) - P_{HV}(\alpha,\beta) \\ &= \frac{1}{2}\cos^2(\alpha-\beta) + \frac{1}{2}\cos^2(\alpha-\beta) - \frac{1}{2}\sin^2(\alpha-\beta) - \frac{1}{2}\sin^2(\alpha-\beta) \\ &= \cos^2(\alpha-\beta) - \sin^2(\alpha-\beta) \\ &= \cos(2(\alpha-\beta)). \end{aligned} \tag{4.35}$$

The correlation function E is the first measurement for proving the violation in terms of the coincidence counts of the outcomes photon pair, all the possible measurement outcomes are varied from $+1$ to -1,

$$E(\alpha,\beta) = \frac{C(\alpha,\beta) + C(\alpha_\perp,\beta_\perp) - C(\alpha,\beta_\perp) - C(\alpha_\perp,\beta)}{C(\alpha,\beta) + C(\alpha_\perp,\beta_\perp) + C(\alpha,\beta_\perp) + C(\alpha_\perp,\beta)}. \tag{4.36}$$

The uncertainty of measuring the correlation function E is given by,

$$(\Delta E(\alpha,\beta))^2 = \frac{1 - E(\alpha,\beta)}{C(\alpha,\beta) + C(\alpha_\perp,\beta_\perp) + C(\alpha,\beta_\perp) + C(\alpha_\perp,\beta)} \tag{4.37}$$

The second measurement considered by the CHSH Inequality is the quantity S , which can be obtained by constraining the correlation function E by using four angles combination;

$$S = |E(a,b) - E(a,b')| + |E(a',b) - E(a',b')|, \tag{4.38}$$

where the notations a, a', b, b' are four different polarisers angles.

S is proved by the local HVT to be equal to 2 and soon after determining by CHSH to be:

$$|S| \leqslant 2 \tag{4.39}$$

The theoretical limit of the violation of CHSH inequality with the choice of certain angles must be equal to,

$$S = 2\sqrt{2} \tag{4.40}$$

The standard deviation of the calculated S is given by,

$$\Delta S = \sqrt{\sum_{a=\alpha,\alpha'} \sum_{b=\beta,\beta'} \Delta E(a,b)^2} \tag{4.41}$$

The next section will discuss how to measure the fidelity of entangled system.

4.3 Fidelity of Polarised Entangled System

The purity of the generated entangled photon pair can be achieved by determining the fidelity of the system. The fidelity is realised by obtaining the density matrices of pair of the entangled photons (qubits) after considering the interference effect of entangled photons, which has been attained through the Hong-Ou-Mandel interference effect.

4.3.1 Hong-Ou-Mandel Effect

The interference of two photons directed towards a non-polarising beam splitter (interferometer) is illustrated by the effect of Hong-Ou-Mandel. This is the phenomena applied for testing the degree of indistinguishably of two incoming photons is demonstrated by C. K. Hong, Z. Y. Ou and Leonard Mandel in 1987 (Hong *et al.*, 1987).

When two photons (A and B) enter a 50 : 50 beam splitter, see Fig. (4.5), there are four possible behavior for theses photons :

1) Photon A is reflected and photon B is transmitted.

2) Both of the photons (A and B) are transmitted.

3) Both of photons are reflected.

4) Photon A is transmitted and the photon B is reflected.

Fig. (4.6), shows the HOM dip for two photons interference, which is firstly observed by using visible-light photon pair generated in a nonlinear crystal via parametric down-conversion. The indistinguishability of the photons can be tested by using two detectors to detect the photon pairs after they passed through beam splitter, the out coming photons register in coincidence. The incoming photons will be completely indistinguishable, if they have the same wavelength, polarisation and spatial-temporal mode, which

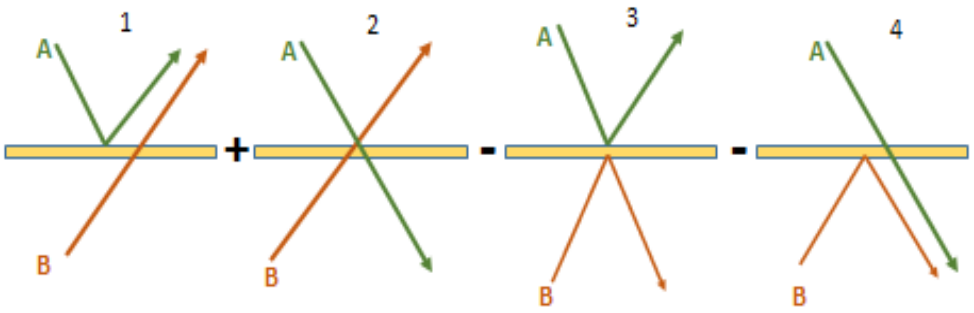


FIGURE 4.5: Hong-Ou-Mandel interference for two photons. 1) the photon A is reflected and photon B is transmitted, 2) Both of the photons (A and B) are transmitted, 3) Both of photons are reflected, 4) Photon A is transmitted and the photon B is reflected.

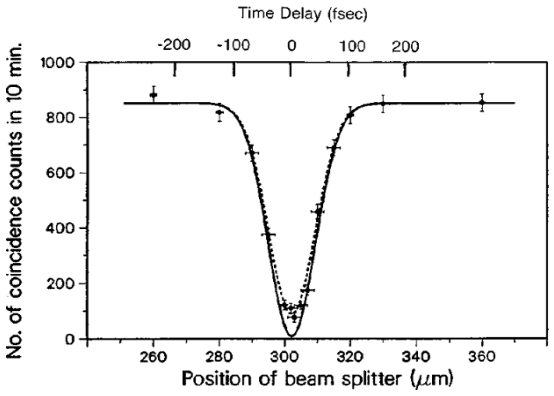


FIGURE 4.6: Hong-Ou-Mandel dip illustrated the coincidence counts vs the relative delay for single photon interference (Mandel (1999))

realised in the case of zero coincidence counts when the dip, almost reaches the zero. while the incoming photons are distinguishable in case of no-dip (Mandel, 1999)

The interference of the generated photon pair applied for testing the fidelity of the entangled photon pair system. Experimentally the distinguishability of the photon pairs, obtained via a balanced beam-splitter instead of constructing a traditional interferometer. This by making use of a fused 50 : 50 polarisation maintaining beam splitter.

The output of the 50 : 50 polarisation maintaining beam splitter was connected via a receiving collimator to the coincidence counter in order to measure the coincidence. Using the aforementioned interferometer a state tomography can be performed

to reconstruct the density matrix of an unknown quantum state.

4.3.2 Tomographic reconstruction of quantum states

Quantum state tomography is a very useful method to achieve the quantum state of the system. The reconstruction of a quantum state through quantum state tomography is realised by using a set of pre-defined projective measurements on a collective identically prepared particles.

In this experiment, the state tomography (tomographic reconstruction) applied to measure the fidelity of the entangled system by reconstructing the density matrix, which is linearly related to a set of 16 projective measured quantities for the entangled photon pairs. The fidelity F of the system can be measured through the following relation;

$$F = Tr[(\sqrt{\rho_{\text{th}}}\rho_{\text{exp}}\sqrt{\rho_{\text{th}}})^2], \tag{4.42}$$

where ρ_{exp} is the experimental density matrix that is obtained by the state tomography, ρ_{th} is the theoretical density matrix. The value of the fidelity of the system varies from 0 to 1 (Altepeter *et al.*, 2005).

To satisfy the indistinguishability condition the value of the fidelity must equal 1 and is obtained when $\rho_{\text{th}} = \rho_{\text{exp}}$. The number of the coincidence counts C_ν observed during the experiment is determined by;

$$C_\nu = \mathcal{C}\langle\psi_\nu|\hat{\rho}\,|\psi_\nu\rangle\,, \tag{4.43}$$

where $\hat{\rho}$ represent the tomographic reconstructed density matrix (experimental density matrix) for the entangled photon pair, $\mathcal{C}$ is the total number of the coincidence counts and $|\psi_\nu\rangle$ is the projection measurement.

4.3.3 The Set of Projection Measurements

The number of projections required for measurements of two polarised photons can be realised by the Stokes parameters S_i, with his four parameters that allow to determine the polarisation state of a light beam (Stokes, 2009), the stokes parameters for single

qubit are defines as follow,

$$\begin{aligned} S_0 &\equiv 2n_0 = \mathcal{N}(\langle R|\hat{\rho}|R\rangle + \langle L|\hat{\rho}|L\rangle), \\ S_1 &\equiv 2(n_1 - n_0) = \mathcal{N}(\langle R|\hat{\rho}|L\rangle + \langle L|\hat{\rho}|R\rangle), \\ S_2 &\equiv 2(n_2 - n_0) = \mathcal{N}i(\langle R|\hat{\rho}|L\rangle - \langle L|\hat{\rho}|R\rangle), \\ S_3 &\equiv 2(n_3 - n_0) = \mathcal{N}(\langle R|\hat{\rho}|R\rangle - \langle R|\hat{\rho}|R\rangle), \end{aligned} \tag{4.44}$$

where S_0, S_1, S_2 and S_3 are the Stokes parameters, n_0, n_1, n_2 and n_3 are the number of photons counted by detector, $\mathcal{N}$ is constant depend on the detector efficiency and the light intensity and R and L are the right and left -handed circular states.

For reconstructing the quantum state of a system composed of two qubits, here we use the 2-photon Stokes parameters S_{i_1,i_2} that is defined in an anlagous manner in single photon Stokes paramenters that defined in Eq. (4.44). The S_{i_1,i_2} can be calculated from the qubit measurement operaters $\hat{\mu}_i$ and Pauli operators σ_i together with the total number of the coincidence counts C (James *et al.*, 2001). These parameters also characterise the density matrix. This density matrix can be written in terms of a superposition of the two-qubit Pauli matrices $\hat{\sigma}_{i_1} \otimes \hat{\sigma}_{i_2}$, weighted by the Stokes parameters S_{i_1,i_2}. It is given by,

$$\hat{\rho} = \frac{1}{4} \sum_{i_1,i_2}^{3} \frac{S_{i_1,i_2}}{S_{0,0}} \hat{\sigma}_{i_1} \otimes \hat{\sigma}_{i_2}, \tag{4.45}$$

where $S_{0,0}$ is a normalisation factor. The $\hat{\sigma}_i$ matrices are defined as;

$$\hat{\sigma_0} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \hat{\sigma_1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma_2} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \hat{\sigma_3} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4.46}$$

For a single qubit, the measurement for a quantum state tomography by four set of projection measurements operators $\hat{\mu}_0$, $\hat{\mu}_1$, $\hat{\mu}_2$, $\hat{\mu}_3$ suffice to reconstruct the state in the Horizontal, Vertical, Diagonal, Right circular and Left circular polarisation components [H, V, D, R,L].

In case of two qubits, the state can be determined by the set of 16 measurements represented by the measurement operators $\hat{\mu}_i \otimes \hat{\mu}_j$ $(i, j = 0, 1, 2, 3)$ (4^n) (n is the number of the qubits) Fig. (4.7).

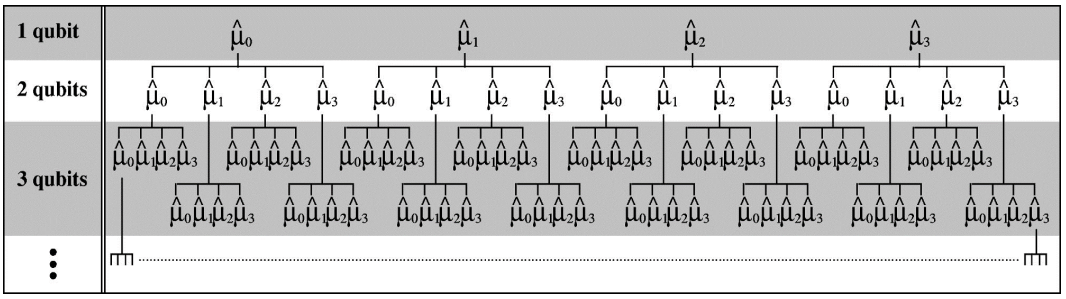


FIGURE 4.7: The tree diagram for determining the required measuring projection for n-number of qubits (James *et al.*, 2001).

To obtain the coincidence counts for the 16 projections, the pump beam was projected onto a polarisation state by using three optical elements (polariser, a Quarter-Wave Plate (QWP), and a Half-Wave Plate (HWP)), which are placed facing each of the down converted photon pairs in front of each detector. The polariser allows transition of only vertically polarised light, while the wave plates angles set randomly, allow the μ ν projection polarisation state to be stable.

The possible combination of projecting the two photons into either H, V plus diagonal P or right circular R states is defined with 4×4 matrices $\hat{\Gamma}_\nu$ and $\hat{\Gamma}_\mu$, where $\nu, \mu =$ H, V, D, L, R, which notate for H =horizontal, V =vertical, D= diagonal, L=left-handed circular and R= right-handed circular. The D, R and L are polarisation states resulting from the superposition of H and V, by using the notation following James *et al.* (2001) for this section, the projections are given by,

$$|H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{4.47}$$

The states D and R are defined, respectively, as ;

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle). \tag{4.48}$$

$$|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i\,|V\rangle). \tag{4.49}$$

$$|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i\,|V\rangle). \tag{4.50}$$

The density operator defined as summation of $\hat{\Gamma}_\nu$ matrices and r_ν, which is given by,

$$\hat{\rho} = \sum_{\nu=1}^{16} \hat{\Gamma}_\nu r_\nu. \tag{4.51}$$

r_ν is the νth element of the 16- element column vector that represent the projection. The element of the vector r_ν, is given by:

$$r_\nu = \mathrm{Tr}(\hat{\Gamma}_\nu.\rho). \tag{4.52}$$

The coincidence counts C_ν measured for the entangled photon pairs illustrate a linear relation with the element of the vector r_ν, by using Eq. (4.43) C_ν, are given as;

$$C_\nu = \mathcal{C} \sum_{\mu=1}^{16} B_{\nu,\mu} r_\mu. \tag{4.53}$$

In which $\mathrm{Tr}\left(\hat{\Gamma}_\nu, \hat{\Gamma}_\mu\right) = \delta_{\nu,\mu}$, $\mathcal{C} = \sum_{\nu=1}^{4} C_\nu$ is the total numbers of counts and $B_{\nu,\mu}$ is 16×16 matrix, defined as:

$$B_{\nu,\mu} = \langle \psi_\nu | \hat{\Gamma}_\mu \, | \psi_\nu \rangle \, . \tag{4.54}$$

$$r_\nu = (\mathcal{C})^{-1} \sum_{\mu=1}^{16} (B^{-1})_{\nu,\mu} n_\nu. \tag{4.55}$$

By introducing 4×4 matrix $\hat{M}_\nu$ to help in compacting the reconstruction for the density operator and to obtain the coincidence counts for the 16 projections, which based on tensor products of the complete set of Pauli matrices, is represented by,

$$\hat{M}_\nu = (B^{-1})_{\nu,\mu} \hat{\Gamma}_\mu. \tag{4.56}$$

The reconstructed density matrices for 16 projections can be obtained by substituting Eq. (4.55) into Eq. (4.51) and by using Eq. (4.56). The density matrix $\hat{\rho}$ can be given as;

$$\hat{\rho} = \frac{\sum_{\nu=1}^{16} \hat{M}_\nu C_\nu}{\sum_{\nu=1}^{4} C_\nu}. \tag{4.57}$$

The Fidelity of the entangled system that obtained in Eq. (4.42) can be determined by substituting the density operator or the experimental density matrix in Eq. (4.57) into Eq. (4.42).

Chapter 5

Experimental Realisation

The theoretical background was introduced in the previous chapter, here, we will provide the experimental procedure, results and discussion.

Our experiment is based on the polarisation degree of freedom, since it has been the most well defined in free - space system. The experimental work was based on generating and characterising a polarised entangled single photon source. This was established in four parts: Starting with the experimental setup to create and detect a polarised entangled photon pairs. This was achieved by using a linearly polarised diode laser beam to pump a nonlinear BBO crystal. The detection was realised with single photon counting module based on single photon avalanche detectors.

We performed two tests to verify the entanglement. The first experiment was done by testing the correlation between the entangled photon in two different basis. The second analysis was to violate the CHSH inequality to prove the existence of the entangled photons.

Finally, the purity of the polarised entangled state was tested by measuring the fidelity of the system. The fidelity was determined by reconstructing the density matrix via the quantum state tomography.

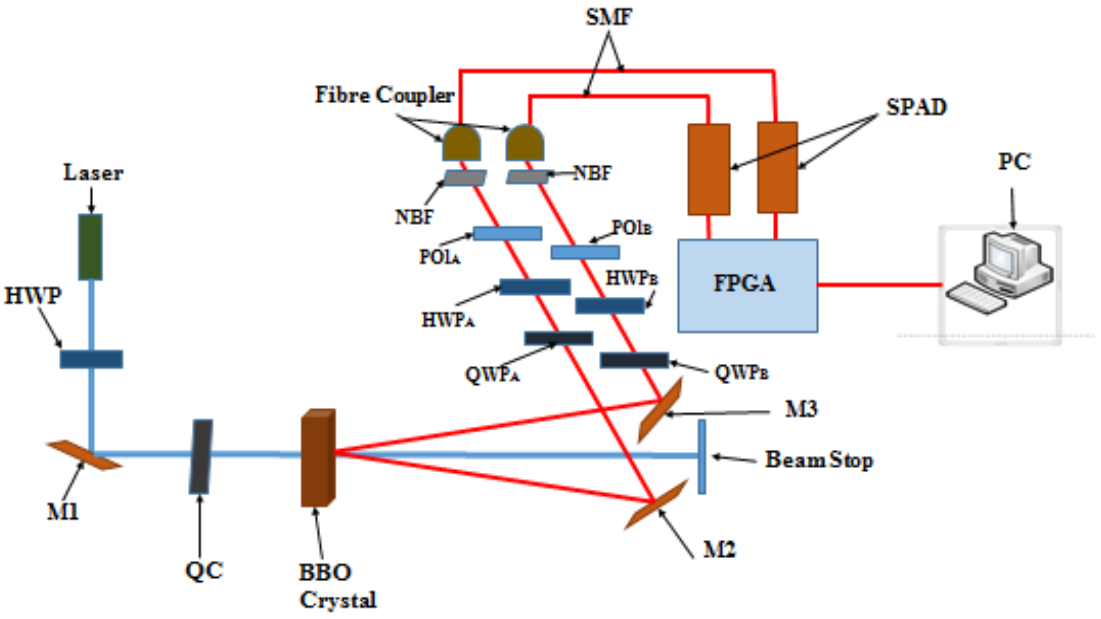


FIGURE 5.1: Optical design of entanglement source consist of 405 nm pump laser, pumped through a Half Wave Plate (HWP), mirror (M1), Quartz Crystal (QC) and BBO non-linear crystal. Entangled photon pairs directed towards into two arms with two mirrors (M2,M3), each arm contain a Quarter Wave Plates (QWP_A, QWP_B), Half Wave Plates (HWP_A, HWP_B), Polarisers (PoL_A, Pol_B), Narrow Band Filter (NBF), Fibre coupler, Single Mode Fibre (SMF), Single Photon Avalanche Detector (SPAD) and the photons will registered as coincidence in FPGA. The coincidence will send to Personal Computer (PC) for counting.

5.1 Experimental setup

For our experiment, the optical system to generate entangled photon pairs consists of a UV diode laser ($\lambda = 405nm$), half wave plate and two concatenated BBO crystals which were cut to demonstrate type-I down conversion. A polariser, a half wave plate and a quarter wave plate were placed in each arm of the down converted photons are used for the projection measurements. A fibre coupler collected the entangled photons, which was transfered to the Single Photon Avalanche Detectors (SPAD) to register the photons as electric pulses. These electric pulses were registered as coincidence counts by using the Field Programming Gate Array (FPGA). For the purpose of the alignment process we used a mirror and fibre coupler laser as illustrates in the optical setup in Fig. (5.1).

5.1.1 Preparing a Pair of Polarised Entangled Photons

The generation of the entangled photon pairs for entanglement system was obtained by using a laser to pump the photons. These photons were directed to the BBO crystal to create the entangled photons.

5.1.1.1 The laser

In our study we used a UV diode laser with a wavelength of $405nm$ and $150mw$ optical output power. This laser has high energy. Because the laser is produced by a diode, then all the photons will have the same polarisation.

A half wave plate was placed after the laser and adjusted to $22.5°$ to give an equal superposition for the horizontal and vertical polarisation. This beam passed through the crystal which created down converted photon pairs.

5.1.1.2 Type-I BBO Crystal

The polarised entangled photon pairs were generated by a BBO crystal which was the medium for the SPDC, that was discussed in Section. (4.1.2). Two crystals were cut for type-I down conversion, mounted orthogonal such that, each one of them was responsible to generate one type of the rectilinear polarisation (horizontal, vertical), as illustrated in Fig. (5.2). The entangled photon pairs emerged with an equal probability of the horizontal, vertical polarisation.

The wavelength of the emerging photons from the BBO crystal was double ($810nm$) compared to the wavelength of the pump beam ($405nm$). This was because of energy conservation. The polarisation of these photons was entangled, such that they will have the same polarisation.

The birefringence of the BBO crystal and the condition of the phase matching forces the entangled photons to propagate in cone shape with circular cross section around the pump beam direction. Those photons emerge with the same energy which was half of the pump beam energy.

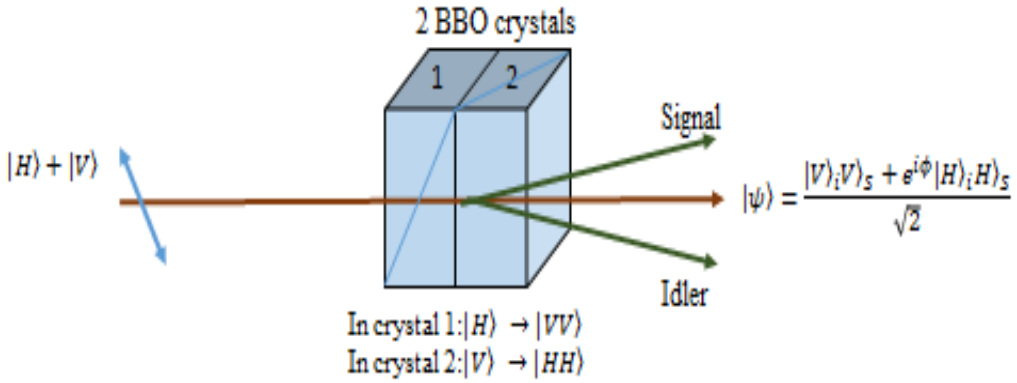


FIGURE 5.2: Two BBO crystal are cut to obtain type-I down conversion. The entangled photon pairs will emerge with 50% probability with horizontal, vertical polarisation.

The phase matching angle for type-I down conversion was set to produce entangled photon pairs by creating an angle of $\pm 3^{\circ}$ with the pump beam direction. To satisfy the condition of conserving the momentum during the SPDC, the down converted photons were emitted in opposite position points in the emitted cone. The crystal was mounted on a rotating stage, which assisted to adjust the crystal optical axis to be in a horizontal plane.

To measure the polarisation state for the down converted photons optical equipments such as polarisers and wave plates were added, which is discussed in the next section.

5.1.2 Polarisers and Wave plates

The polariser is an optical filtering device, which produces a linearly or circularly polarised light from unpolarised light and also has the ability to block certain polarisations. A polariser was placed in each arm of the entangled photon to measure the polarisation state of the entangled photons.

The wave plates are optical devices consisting of uniaxial birefringent crystal. The wave plates change the polarisation state of the light passing through them, by altering the phase between two perpendicular polarisation components of that light.

FIGURE 5.3: Qarter Wave Plates (right) and Half Wave Plate (left) were used to vary the polarisation, and to obtain the coincidence counts for various projective measurements.

Two popular types of the wave plate are half wave plate and quarter wave plate, as shown in Fig. (5.3).

The HWP ($\lambda/2$) transfers the linear polarisation of a light by an angle π and the phase shift between the extraordinary and the ordinary modes is introduces by the same aforementioned angle. The HWP is shown in Fig. (5.3) (left).

The QWP ($\lambda/4$) transfers the linear polarisation to circular polarisation and vice versa, and introduces a phase shift of an angle π^2. The QWP is shown in Fig. (5.3) (right).

In our experiment, we used Thorlab motorized precision rotation stages (PRM1Z8E) to mount the wave plates and the polariser. The PR1Z8E was small, compacted size with $23mm$ thickness and the motor can rotated continuously with 360°. The angular displacement can been measured by the Vernier dial, which was marked on the rotating plate.

The PRM1Z8E stages were driven by the Thorlab TDC001 servomotor driver which was controlled by personal computer with its APT software or by LabVIEW as third party software, see Fig. (5.4).

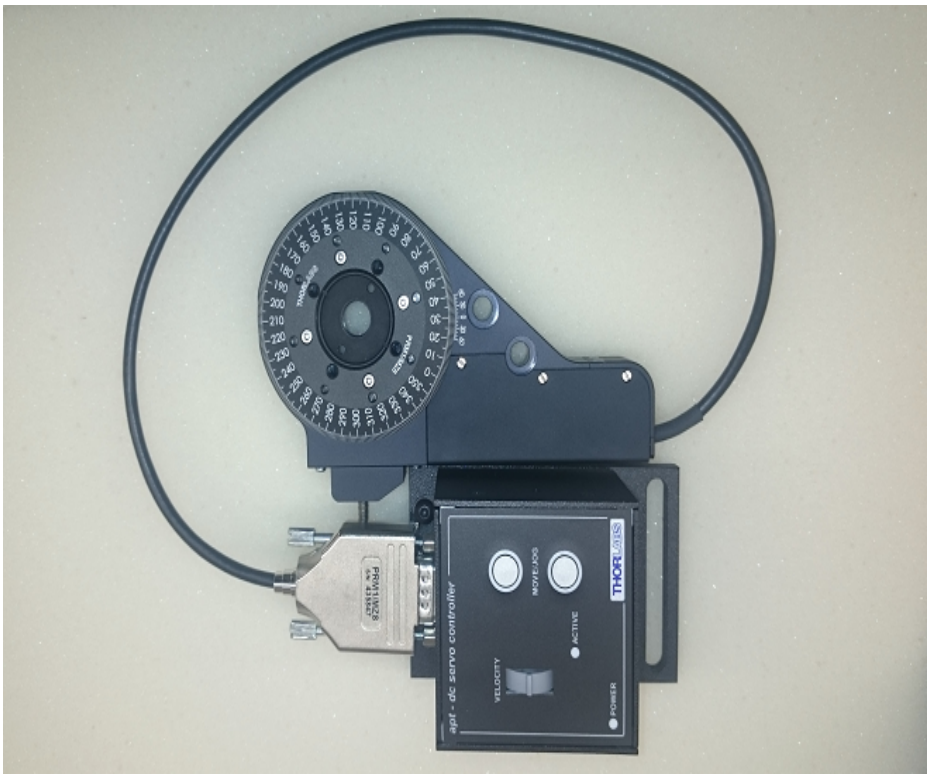


FIGURE 5.4: Thorlab motorized precision rotation stage used to mount the wave-plates as well as the polarisers.

The LabVIEW was coded by following the steps provided in the APT guide to labview.

5.1.3 The collection of the entangled photons

The entangled photon pairs were collected by fibre coupler lenses which transfered the single photons to single mode fibre. Two fibre couplers were chosen to couple a single mode of the polarisation bases for specific wavelength.

These couplers were placed in each arm of the output of the crystal to collect the entangled photon pairs which was transfered to the detector.

The alignment of the fibre couplers were achieved by using the method of the back alignment. In this method, a fibre coupler red laser was plugged on the output of the single mode fibre coupler. We directed the red laser beam through the BBO crystal and by tilting the lens of the fibre coupler adjusted the phase matching angle.

FIGURE 5.5: Two Single Photon Avalanche photodiode Detectors (SPAD) were connected to fibre couplers with Single Mode Fibre (SMP). SMP were collected the down converted photons to be converted into electric signal in SPAD .

The signal was transfered through the fibre coupler to Single Photon Avalanche Detector (SPAD), the next section contain a more detail about the SPAD.

5.1.4 Single Photon Avalanche Detector

Single Photon Avalanche Detector (SPAD) is a compact semiconductor electric device with high efficiency up to 60% for the $810nm$ wavelength, low dark count noise and low electrical power consuming. SPAD has the ability to detect the photon number range from few hundred to 30 million photons per second, and that is by using the technique to measure very weak avalanches pulses at the early period when running the experiment.

The principle behind the SPAD operation is based on converting the energy of the incident photon to free electric charge in semiconductor material by the concept of the photoelectric effect. The output electric signal from the avalanche photodiode is proportional to the number of the incident photon pulses.

The experiment was implemented in dark room due to the sensitivity of these detectors to the background light, in the case when the background light is high, the detection goes above the threshold and that may cause damage to the detectors. For the best performance, the detector was often cooled thermo-electrically to$-30°$C, but it can be used even at room temperature.

In our experiment, we used two SPAD to detect the down converted photons, see Fig. (5.5). The output electrical pulses from the SPAD were connected to the coincidence count module. We used the Altera DE2 FPGA programmed as a counting module, in which the experiments were based on the coincidence counts to demonstrate the measurements.

5.1.5 Coincidence Counts Unit Using the Altera DE2 FPGA

The simultaneous detection of two photons in different detectors is defined as coincidence count. The direct method for counting the coincidence is to use logical AND gates. The pulses from the two detectors are sent to the inputs of AND logic gates and the output of the gate is logically true if and only if both inputs are simultaneously high and the signals must arrive at the same time. The coincidence counting unit was responsible to measure the coincidence. In our experiment this was based on the programmable logic integrated circuit FPGA.

Our Coincidence-Counting Unit (CCU) is a multi-channel CCU built of integrated circuit components. Two signals from the SPAD registered as inputs in the coincidence counting unit, which registered a combination of random 2-fold coincidences. The coincidence window was opened in a very short period $8ns$. The pulses registered in two outputs into a field programmable gate array (FPGA), the coincidence counts for integration time intervals of 1 s .

FPGA is a hardware integrated circuit (chip of semiconductor material) configured by software pre-written in VDHL language. This language was used to control the quantum signal and to tell the machine which gate and module to register the incoming signals from the SPAD detector and how to output the results. The FPGA is high speed and high sensitivity with low dark noise / low excess noise, see Fig. (5.6).

5.1.6 Taking Data

Once all the aforementioned equipment were aligned properly, it was possible to count the coincidence data from the FPGA, and this data was transfered to a personal computer via a USB, which was interfaced by using LabVIEW.

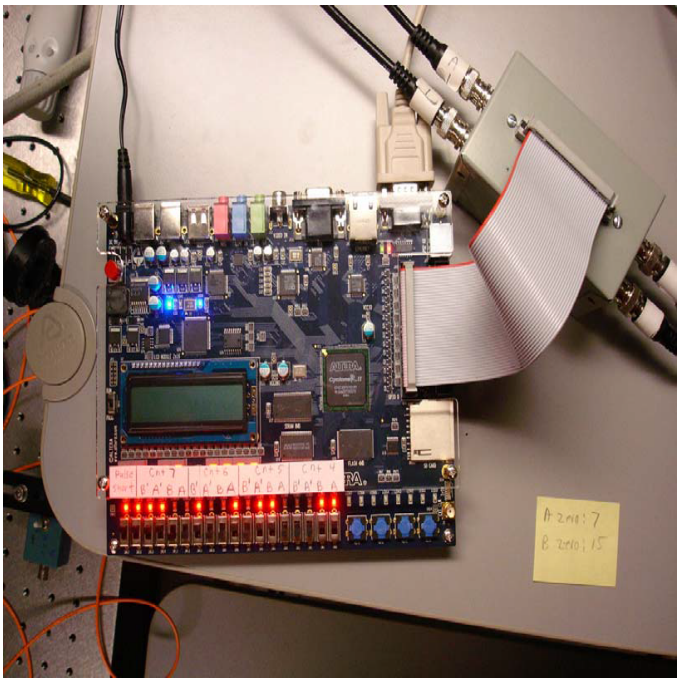


FIGURE 5.6: Field Programmable Gate Array (FPGA) is a coincidence counts module that detect the incoming signal from the SPAD to register it as coincidence.

LabVIEW (short for Laboratory Virtual Instrumentation Engineering Workbench) is a graphical programming language from National instruments. It uses icons instead of lines of codes to create an environment to run a certain applications. LabVIEW uses dataflow programming, in which the data flow determines the execution.

LabVIEW program is also known as Virtual Instrument (VI), since it has the ability to operate as a physical instrument. VI uses functions to display an input from the user interface or other sources and present the information in computer files. VI consist of three components: a) the front panel, which is the user interface, that is built of a set of tools and objects. b) The code or the block diagram which is used to control the front panel by adding graphical representations of functions. c) Icons and connector pane, classifies the VI. Also, the VI has the property to be used inside another VI, which is called a subVI.

In our study, we used LabVIEW code for the coincidence counts written by Mark Beck. We have modified it in order to be compatible to our equipments.

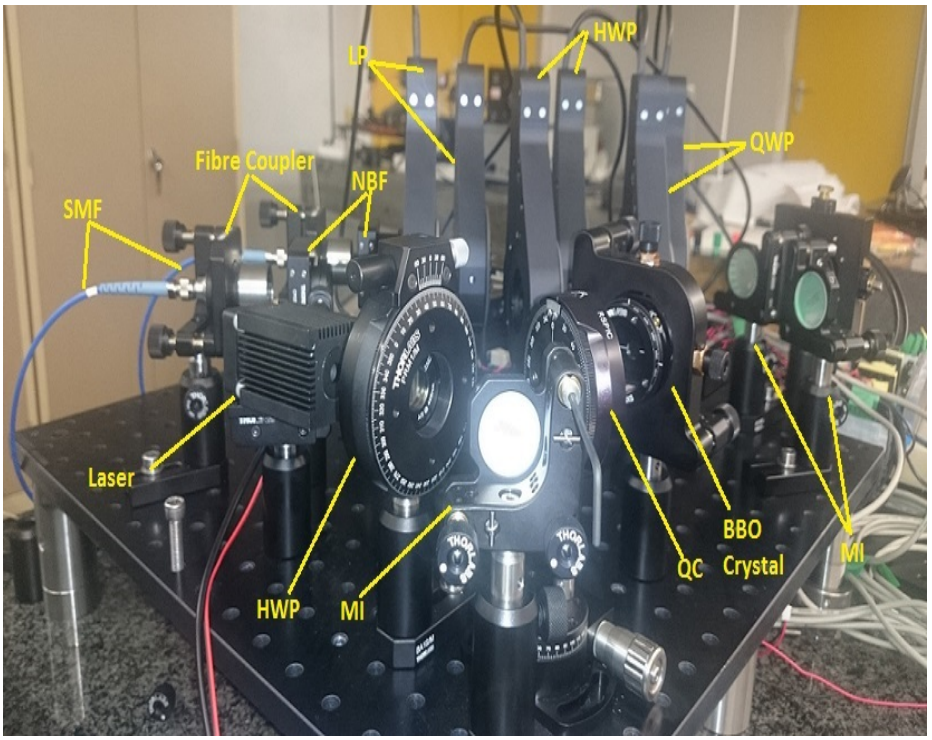


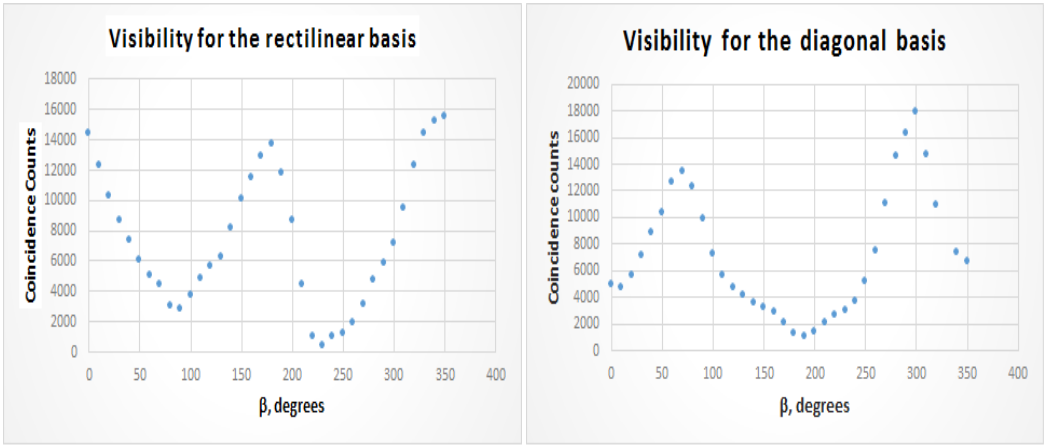
FIGURE 5.7: Figure illustrated the final alignment of the equipments which used to test the visibility, CHSH inequality and the fidelity of the system. A 405 *nm* laser has pumped through a Half Wave Plate (HWP), mirror (MI), the phase difference of the polarisation of the pump beam is adjusted with Quartz Crystal (QC), the pump beam photons directed toward a BBO non-linear crystal which is the medium for SPDC. The entangled photon pairs emerge from the BBO crystal and directed to arms two mirrors, each arm contain a Quarter Wave Plates (QWP), Half Wave Plates (HWP), Polarisers (PoL), Narrow Band Filter (NBF), Fibre coupler to collect the entangled photons, Single Mode Fibre (SMF) to transfer the entangled photon pairs to Single Photon Avalanche Detector (SPAD). The photons will registered as coincidence in FPGA, and the coincidence will send to Personal Computer (PC) for counting.

5.2 The correlation Measurements

The optical equipments used to test the correlation of the entangled photons were illustrated in Fig. (5.7) and Fig. (5.5) and the HWP and QWP were set to 0°. This correlation was tested by measuring the visibility of the rectilinear and diagonal bases, and by violating the CHSH inequality.

5.2.1 The Visibility

In order to test the visibility of the entangled photon pairs in the two non-orthogonal bases (the rectilinear and the diagonal bases), two polarisers were adjusted. The angle of the first polariser was set to 0° degree for the rectilinear bases, and 45° for the diagonal



(A) Rectilinear basis (B) Diagonal basis

FIGURE 5.8: Plot illustrating the polarisation correlation between the rectilinear and diagonal bases. Fig. (5.8a) shows the measured coincidence counts for different polarisations in the rectilinear basis. Fig. (5.8b) represents the measured coincidence counts for different polarisations in the diagonal basis.

basis and by changing the orientation of the second polariser and by measuring the coincidence by the FPGA, the the visibility were obtained. The outcomes coincidence counts were plotted against the different angles of the second polariser, which allowed us to test the correlation and the existence of the entangled photons by observing the cosine square dependence .

The coincidence counts for two non-orthogonal bases were observed as illustrated in Fig. (5.8), which demonstrated a cosine square dependence and proves the existence of the entangled photons.

The visibility was measured by using Eqn. (4.33) and Eqn. (4.34) to be 94 ± 0.016 for the rectilinear basis, and 90 ± 0.013 for the diagonal basis, and this verified the strong correlation and demonstrated the non-classical behaviour of the entangled photon pairs.

5.2.2 CHSH Inequality Violation

We also used the same optical setup to violate the CHSH inequality. This was demonstrated by measuring the coincidence counts of the polarised entangled photon pairs after each had passed through polariser analyser. Here, we used different angle orientations for the two polariser (polariser A with an angle α, polariser B with an angle β). The correlation function E was measured by running four different angles setting for each

TABLE 5.1: Coincidence counts data for violating CHSH inequality experiment with different polarisations angles and with integration time 1s and accidental coincidence=8%.

α	β	$C(\alpha,\beta)$
0	22.5°	9841
90°	22.5°	903
0°	112.5°	1476
90°	112.5°	9702
45°	22.5°	11911
135°	22.5°	370
45°	112.5°	2122
1355°	122.5°	4588
0	67.5°	711
90°	67.5°	7706
0	157.5°	10263
90°	157.5°	2890
45°	67.5°	12171
135°	67.5°	350
45°	157.5°	3173
135°	157.5°	4667

polariser, $(\alpha, \alpha', \alpha_\perp, \alpha'_\perp)$ and $(\beta, \beta', \beta_\perp, \beta'_\perp)$. The resulted 16 coincidence counts rates represented in Table. (5.1).

The expectation value E was measured using the 16 coincidence counts given in Table. (5.1). After we applied Eqn. (4.36), we obtained the different values of E for different polarisations as follows,

$E(0, 22.5°)$=0.78 ± 0.002

$E(45°, 22.5°)$=0.74 ± 0.003

$E(0, 67.5^{\circ})$=-0.67 ± 0.003

$E(45°, 67.5^{\circ})$=0.65 ± 0.003

The quantity S is calculated according to Eqn. (4.38) to be 2.80 ± 0.011.

The above mentioned results violate the CHSH inequality and provided strong evidence, that our system was described by quantum theory.

TABLE 5.2: The coincidence counts data measured in different polarisation projection to reconstruct the density matrix.

State v	HWP 1	QWP 1	HWP 2	QWP 2	C
$v = 1\ \|H\rangle\ \|H\rangle$	45°	0	45°	0	30101
$v = 2\ \|H\rangle\ \|V\rangle$	45°	0	0	0	818
$v = 3\ \|V\rangle\ \|V\rangle$	0	0	0	0	39653
$v = 4\ \|V\rangle\ \|H\rangle$	0	0	45°	0	594
$v = 5\ \|R\rangle\ \|H\rangle$	22.5°	0	45°	0	8392
$v = 6\ \|R\rangle\ \|V\rangle$	22.5°	0	0	0	12014
$v = 7\ \|P\rangle\ \|V\rangle$	22.5°	45°	0	0	17205
$v = 8\ \|P\rangle\ \|H\rangle$	22.5°	45°	45°	0	11508
$v = 9\ \|P\rangle\ \|R\rangle$	22.5°	45°	22.5°	0	14070
$v = 10\ \|P\rangle\ \|P\rangle$	22.5°	45°	22.5°	45°	22680
$v = 11\ \|R\rangle\ \|P\rangle$	22.5°	0	22.5°	45°	9589
$v = 12\ \|H\rangle\ \|P\rangle$	45°	0	22.5°	45°	10774
$v = 13\ \|V\rangle\ \|P\rangle$	0	0	22.5°	45°	7288
$v = 14\ \|V\rangle\ \|L\rangle$	0	0	22.5°	90°	8896
$v = 15\ \|H\rangle\ \|L\rangle$	45°	0	22.5°	90°	13064
$v = 16\ \|R\rangle\ \|L\rangle$	22.5°	0	22.5°	90°	31007

5.3 Fidelity of the System

The fidelity of the system was measured by reconstructing the density matrix via the quantum state tomography, as discussed in Section. (4.3.2).

To observe 16 coincidence counts for 16 projection measurements were performed by adjusting the orientation of HWP and QWP as shown in Table. (5.2).

The density matrix was reconstructed for 16 projective polarisations state which are given in Table. (5.2). From Eqn. (5.1) ,the reconstructed matrix is normalised with $\mathrm{Tr}\hat{\rho} = 1$ and Hermitian $\hat{\rho}^{\dagger} = \hat{\rho}$. The fidelity of the system was equal to 0.97 ± 0.0003, this value demonstrated the indistinguishbility of the entangled photons. The real part of the reconstructed density matrix is given in the graphical representation shown in Fig. (5.9).

$$\hat{\rho} = \begin{pmatrix} 0.4229 & 0.0337i - 0.0659 & -0.0978i - 0.0540 & 0.0147i + 0.6281 \\ -0.0337i - 0.0658 & 0.0115 & 0.3392i - 0.2730 & -0.1155i - 0.0426 \\ 0.0977i - 0.05395 & -0.3392i - 0.2730 & 0.00835 & 0.1578i - 0.1803 \\ 0.6281 - 0.0147i & 0.1040i - 0.0426 & -0.1578i - 0.1804 & 0.55719 \end{pmatrix} \tag{5.1}$$

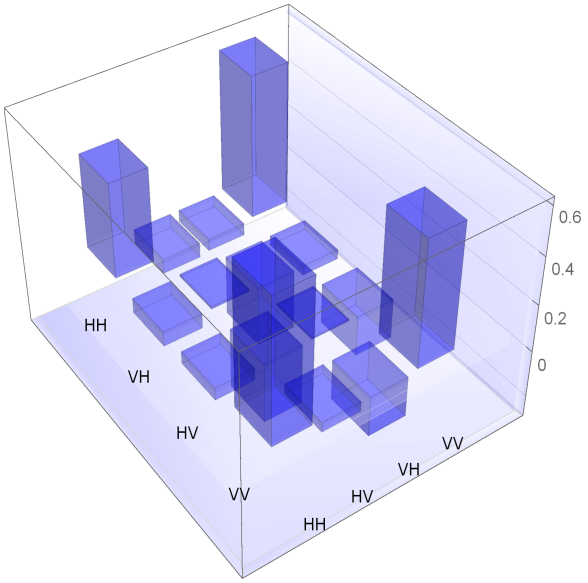


FIGURE 5.9: Graphical representation of the real part of the density matrix that reconstructed in the above results.

Chapter 6

Conclusion

Quantum theory was originally developed to describe the smallest entities in physics. Later it turned out that it also makes fascinating predictions over macroscopic distances. Establishing quantum technology as an application in quantum information science enables quantum systems to become available as a resource for communication protocols such as Quantum Key Distribution (QKD), for both fibre and free space system.

QKD has been considered as a field of research that uses quantum mechanical principle to transfer the information between parties. QKD based entanglement is a communication protocol that produces a higher layer in the security of the information. The successful implementation of such protocol, is based on the transmission and detection of entangled photons, would validate the key technology of a quantum communications protocol.

Although the development in the present technologies such as quantum optics and fibre optic technology had implemented the privacy tasks of the QKD, there are some factors reduces the security of the QKD based entanglement. It involves the equipment efficiencies, decoherence of the entangled photons and the coincidence collections efficiency. It also limits the rate of producing a good quality of entangled photons as well as the security of the QKD.

This thesis has given a brief outline of quantum entanglement and it is application in QKD and explained the method of producing entangled photon pairs. The detection of good quality entangled states was also a part of this study. Furthermore, it represented experimental results on some tests have been done to characterise the system for QKD.

This project was undertaken to design an automated, portable system that generated efficient polarised entangled photon pairs, which can be used to develop the quantum communication-based entanglement such as QKD. Our system demonstrated the fundamental features that important to implement the privacy task for QKD based entanglement. We started by producing efficient entangled photons that are providing a high rate for transforming the information, this was established by using Spontaneous Parametric Down Conversion (SPDC) process.

Afterwards, the correlation was tested by measuring the visibility of the system in two different bases (rectilinear and diagonal basis). The resulting values illustrate the strong correlation of our entangled photons. Also, the Clauser, Horne, Shimony and Holt (CHSH) inequality was violated to prove the existence of the entangled photons. Violating the CHSH inequality demonstrates the non-classical correlation of these photons and the strong evidence of non-locality of nature.

Finally, the purity of our system has been established by carrying out the quantum state tomography technique and reconstructing the density matrix to measure the fidelity of the system.

Many techniques were considered in this study to overcome the decoherence and the coincidence collection efficiency limitations. This was obtained by using type-I ultra-bright β Barium BOrate (BBO) crystal as medium for SPDC together with crystal compensator. These two are used to increase the brightness of type-I source and that improves the fidelity of the system. Also, by adjusting the relative phase shift between photons of different polarisation in birefringent crystals increase the coincidence collection efficiencies.

Taken all together, our good results suggest that our system can be used to implement the privacy tasks of QKD. The study enhances our understanding in entanglement as phenomena with too many applications in quantum mechanics field area and the quantum information theory. This research will serve as a base for future studies involving QKD in our research group, generating the key and producing the communication protocols in everyday life. The current finding adds to a growing body of literature on the testing fundamental of quantum mechanics with large scale ground spaces and moving frames, involving ground satellite links which is of my interest for future work. The ground satellite links tests are based on link distances exceeding the Low Earth Orbit

(LEO) scale (below 2000 km). Satellites with orbits higher than LEO are interesting for the implementation of secure information protocols for future Global Navigation Satellite System (GNSS) constellations, or for the realisation of permanent links with GEOstationary (GEO) satellites.

Bibliography

J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat. Photonic state tomography. *Advances In Atomic, Molecular, and Optical Physics*, **52**:105–159, 2005.

A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via bell's theorem. *Physical Review Letters*, **47**(7):460, 1981.

M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, and A. Zeilinger. Long-distance quantum communication with entangled photons using satellites. *arXiv preprint quant-ph/0305105*, 2003.

H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A*, **59**(6):4238, 1999.

M. Beck. *Quantum Mechanics: Theory and Experiment*. OUP USA, 2012. ISBN 9780199798124. URL https://books.google.co.za/books?id=r--TbbrYjr8C.

J. S. Bell. On the einstein podolsky rosen paradox, 1964.

J. S. Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, **38**(3):447, 1966.

C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, **68**(21):3121, 1992.

C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, **560**:7–11, 1984.

C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, **70**(13):1895, 1993.

A. Berkley, H. Xu, R. Ramos, M. Gubrud, F. Strauch, P. Johnson, J. Anderson, A. Dragt, C. Lobb, and F. Wellstood. Entangled macroscopic quantum states in two superconducting qubits. *Science*.

D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, **390**(6660):575–579, 1997.

D. Bromley and W. Greiner. *Quantum Mechanics: An Introduction*. Physics and Astronomy. Springer Berlin Heidelberg, 2000. ISBN 9783540674580. URL https://books.google.co.za/books?id=7qCMUfwoQcAC.

D. C. Burnham and D. L. Weinberg. Observation of simultaneity in parametric production of optical photon pairs. *Physical Review Letters.*, **25**:84–87, Jul 1970. doi: 10.1103/PhysRevLett.25.84. URL http://link.aps.org/doi/10.1103/PhysRevLett.25.84.

J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, **23**(15):880, 1969.

M. J. de Dood, W. Irvine, and D. Bouwmeester. Non-linear photonic crystals as a source of entangled photons. *arXiv preprint quant-ph/0409171*, 2004.

D. Dehlinger and M. Mitchell. Entangled photons, nonlocality, and bell inequalities in the undergraduate laboratory. *American Journal of Physics*, **70**(9):903–910, 2002.

D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume **400**, pages 97–117. The Royal Society, 1985.

P. A. M. Dirac. A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, **35**:416–418, 7 1939. ISSN 1469-8064. doi: 10.1017/S0305004100021162. URL http://journals.cambridge.org/article_S0305004100021162.

A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review Letters*, **47**(10):777, 1935.

H. Eisenberg, J. Hodelin, G. Khoury, and D. Bouwmeester. Multiphoton path entanglement by nonlocal bunching. *Physical Review Letters*, **94**(9):090502, 2005.

A. K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, **67**(6):661, 1991.

A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Optics Express*, **15**(23):15377–15386, 2007.

M. Fox. *Quantum Optics: An Introduction: An Introduction*, volume **6**. Oxford university press, 2006.

S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, **28**(14):938, 1972.

E. S. Fry and R. C. Thompson. Experimental test of local hidden-variable theories. *Physical Review Letters*, **37**(8):465, 1976.

G. Gamow. *Thirty years that shook physics: the story of quantum theory*. Science study series. Doubleday, 1966. URL https://books.google.co.za/books?id=lwlRAAAAMAAJ.

J. S. Geller. Lab 1: Entanglement and bell's inequalities.

N. Gisin. Bell's inequality holds for all non-product states. *Physics Letters A*, **154**(5): 201–202, 1991.

N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics*, **74**(1):145, 2002.

O. Goldreich. *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2009.

R. B. Griffiths. *Consistent quantum theory*. Cambridge University Press, 2003.

H. Häffner, W. Hänsel, C. Roos, J. Benhelm, M. Chwalla, T. Körber, U. Rapol, M. Riebe, P. Schmidt, C. Becher, *et al.* Scalable multiparticle entanglement of trapped ions. *Nature*, **438**(7068):643–646, 2005.

B. Hall. *Quantum Theory for Mathematicians*. Graduate Texts in Mathematics. Springer New York, 2013. ISBN 9781461471165. URL https://books.google.co.za/books?id=bYJDAAAAQBAJ.

M. Hayashi, S. Ishizaka, A. Kawachi, G. Kimura, and T. Ogawa. *Introduction to Quantum Information Science*. Graduate Texts in Physics. Springer Berlin Heidelberg, 2014. ISBN 9783662435021. URL https://books.google.co.za/books?id=4gdYBAAAQBAJ.

W. Heisenberg. *The Physical Principles of the Quantum Theory*. Dover Books on Physics and Chemistry. Dover Publications, 1949. ISBN 9780486601137. URL https://books.google.co.za/books?id=NzMBh4ZxKJsC.

L. Helt, Z. Yang, M. Liscidini, and J. Sipe. Spontaneous four-wave mixing in microring resonators. *Optics Letters*, **35**(18):3006–3008, 2010.

C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, **59**:2044–2046, Nov 1987. doi: 10.1103/PhysRevLett.59.2044. URL http://link.aps.org/doi/10.1103/PhysRevLett.59.2044.

R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Reviews of Modern Physics*, **81**(2):865, 2009.

D. F. James, P. G. Kwiat, W. J. Munro, and A. G. White. Measurement of qubits. *Physical Review A*, **64**(5):052312, 2001.

T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. *Physical Review Letters*, **84**(20):4729, 2000.

A. Karlsson, M. Koashi, and N. Imoto. Quantum entanglement for secret sharing and secret splitting. *Physical Review A*, **59**(1):162, 1999.

T. Kuhn. *Black-body theory and the quantum discontinuity, 1894-1912*. Oxford University Press, 1978. URL https://books.google.co.za/books?id=DwQvAAAAIAAJ.

P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih. New high-intensity source of polarization-entangled photon pairs. *Physical Review Letters*, **75**(24):4337, 1995.

N. Lambert, C. Emary, and T. Brandes. Entanglement and the phase transition in single-mode superradiance. *Physical Review Letters*, **92**(7):073602, 2004.

C.-C. Lin. Elasticity of calcite: thermal evolution. *Physics and Chemistry of Minerals*, **40**(2):157–166, 2013.

H.-K. Lo and N. Lütkenhaus. Quantum cryptography: from theory to practice. *arXiv preprint quant-ph/0702202*, 2007.

C. Macchiavello, G. Palma, and A. Zeilinger. *Quantum Computation and Quantum Information Theory: Reprint Volume with Introductory Notes for ISI TMR Network School*. 2001. ISBN 9789814494052. URL https://books.google.co.za/books?id=-2bVCgAAQBAJ.

L. Mandel. Quantum effects in one-photon and two-photon interference. *Reviews of Modern Physics*, **71**:S274–S282, Mar 1999. doi: 10.1103/RevModPhys.71.S274. URL http://link.aps.org/doi/10.1103/RevModPhys.71.S274.

E. Mascarenhas and M. F. Santos. Emergence of classicality in small-number entangled systems. *Physical Review A*, **79**(2):023836, 2009.

K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger. Dense coding in experimental quantum communication. *Physical Review Letters*, **76**(25):4656, 1996.

N. D. Mermin. Is the moon there when nobody looks? reality and the quantum theory. *Physics today*, **38**(4):38–47, 1985.

D. Moskovich. An overview of the state of the art for practical quantum key distribution. *arXiv preprint arXiv:1504.05471*, 2015.

J. V. Neumann. *Mathematical Foundations of Quantum Mechanics*. Investigations in physics. Princeton University Press, 1955. ISBN 9780691028934. URL https://books.google.co.za/books?id=JLyCo3RO4qUC.

M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

Z. Ou and L. Mandel. Violation of bell's inequality and classical probability in a two-photon correlation experiment. *Physical Review Letters*, **61**(1):50, 1988.

J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger. Experimental entanglement swapping: Entangling photons that never interacted. *Physical Review Letters*, **80**(18):3891, 1998.

J.-W. Pan, C. Simon, Č. Brukner, and A. Zeilinger. Entanglement purification for quantum communication. *Nature*, **410**(6832):1067–1070, 2001.

M. Planck. *Introduction to theoretical physics: by Max Planck. Translated by Henry L. Brose.* Number v. 4 in Introduction to Theoretical Physics: By Max Planck. Translated by Henry L. Brose. MacMillan, 1957. URL https://books.google.co.za/books?id=x-APAQAAMAAJ.

M. Planck and H. Kangro. *Planck's original papers in quantum physics: German and English edition.* Classic papers in physics. Taylor and Francis, 1972. ISBN 9780850660609. URL https://books.google.co.za/books?id=ewHnAAAAMAAJ.

S. Popescu and D. Rohrlich. Which states violate bell's inequality maximally? *Physics Letters A*, **169**(6):411–414, 1992.

A. Poppe, A. Fedrizzi, R. Ursin, H. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, *et al.* Practical quantum key distribution with polarization entangled photons. *Optics Express*, **12**(16):3865–3871, 2004.

D. Prutchi. *Exploring Quantum Physics through Hands-on Projects.* Wiley, 2012. ISBN 9781118140666. URL https://books.google.co.za/books?id=HYSQZwEACAAJ.

R. Rangarajan, M. Goggin, and P. Kwiat. Optimizing type-i polarization-entangled photons. *arXiv preprint arXiv:1001.4182*, 2010.

J. Rarity, P. Tapster, E. Jakeman, T. Larchuk, R. Campos, M. Teich, and B. Saleh. Two-photon interference in a mach-zehnder interferometer. *Physical Review Letters*, **65**(11):1348, 1990.

M. Redhead. *Incompleteness, Nonlocality, and Realism: A Prolegomenon to the Philosophy of Quantum Mechanics.* Clarendon Paperbacks. Clarendon Press, 1989. ISBN 9780198242383. URL https://books.google.co.za/books?id=Yt6kUGQH_scC.

M. Reed, J. Randall, R. Aggarwal, R. Matyi, T. Moore, and A. Wetsel. Observation of discrete electronic states in a zero-dimensional semiconductor nanostructure. *Physical Review Letters*, **60**(6):535, 1988.

R. Reichle, D. Leibfried, E. Knill, J. Britton, R. Blakestad, J. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. Wineland. Experimental purification of two-atom entanglement. *Nature*, **443**(7113):838–841, 2006.

R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, **21**(2):120–126, 1978.

V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, **92**(5):057901, 2004.

E. Schrödinger. Probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, **32**:446–452, 10 1936. ISSN 1469-8064. doi: 10.1017/S0305004100019137. URL http://journals.cambridge.org/article_S0305004100019137.

E. Schrödinger. Die gegenwärtige situation in der quantenmechanik. *Naturwissenschaften*, **23**(49):823–828, 1935.

M. Serbyn, Z. Papić, and D. A. Abanin. Universal slow growth of entanglement in interacting strongly disordered systems. *Physical Review Letters*, **110**(26):260601, 2013.

Y. Shih and C. O. Alley. New type of einstein-podolsky-rosen-bohm experiment using pairs of light quanta produced by optical parametric down conversion. *Physical Review Letters*, **61**(26):2921, 1988.

G. G. Stokes. *Mathematical and Physical Papers*, volume **3**. Cambridge University Press, 2009. ISBN 9780511702266. URL http://dx.doi.org/10.1017/CBO9780511702266. Cambridge Books Online.

K. Tamaki and N. Lütkenhaus. Unconditional security of the bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Physical Review A*, **69**(3): 032316, 2004.

P. R. Tapster, J. G. Rarity, and P. Owens. Violation of bell's inequality over 4 km of optical fiber. *Physical Review Letters*, **73**(14):1923, 1994.

R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, *et al.* Entanglement-based quantum communication over 144 km. *Nature Physics*, **3**(7):481–486, 2007.

J. Volz, M. Weber, D. Schlenk, W. Rosenfeld, J. Vrana, K. Saucke, C. Kurtsiefer, and H. Weinfurter. Atom-photon entanglement. *arXiv preprint quant-ph/0511183*, 2005.

E. Waks, A. Zeevi, and Y. Yamamoto. Security of quantum key distribution with entangled photons against individual attacks. *Physical Review A*, **65**(5):052310, 2002.

G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of bell's inequality under strict einstein locality conditions. *Physical Review Letters*, **81**(23): 5039, 1998.

R. F. Werner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Physical Review A*, **40**(8):4277, 1989.

S. Wiesner. Conjugate coding. *ACM Sigact News*, **15**(1):78–88, 1983.

M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013. ISBN 9781107034259. URL https://books.google.co.za/books?id=T36v2Sp7DnIC.

A. Zeilinger. *Dance of the Photons: From Einstein to Quantum Teleportation*. Farrar, Straus and Giroux, 2010. ISBN 9781429963794. URL https://books.google.co.za/books?id=Oykw1_269KsC.

Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel, and J.-W. Pan. Experimental demonstration of five-photon entanglement and open-destination teleportation. *Nature*, **430**(6995):54–58, 2004.